



IJCSIS Vol. 17 No. 5, May 2019
ISSN 1947-5500

International Journal of Computer Science & Information Security

© IJCSIS PUBLICATION 2019
Pennsylvania, USA

Indexed and technically co-sponsored by :



AUTHOR SERIES



Indexing Service

IJCSIS has been indexed by several world class databases, for more information, please access the following links:

Global Impact Factor

<http://globalimpactfactor.com/>

Google Scholar

<http://scholar.google.com/>

CrossRef

<http://www.crossref.org/>

Microsoft Academic Search

<http://academic.research.microsoft.com/>

IndexCopernicus

<http://journals.indexcopernicus.com/>

IET Inspec

<http://www.theiet.org/resources/inspec/>

EBSCO

<http://www.ebscohost.com/>

JournalSeek

<http://journalseek.net>

Ulrich

<http://ulrichsweb.serialssolutions.com/>

WordCat

<http://www.worldcat.org>

Academic Journals Database

<http://www.journaldatabase.org/>

Stanford University Libraries

<http://searchworks.stanford.edu/>

Harvard Library

<http://discovery.lib.harvard.edu/?itemid=|library/m/aleph|012618581>

UniSA Library

<http://www.library.unisa.edu.au/>

ProQuest

<http://www.proquest.co.uk>

Zeitschriftendatenbank (ZDB)
<http://dispatch.opac.d-nb.de/>

IJCSIS

ISSN (online): 1947-5500

Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

CALL FOR PAPERS

International Journal of Computer Science and Information Security (IJCSIS) January-December 2019 Issues

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.

See authors guide for manuscript preparation and submission guidelines.

Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Scopus Database, Cornell University Library, ScientificCommons, ProQuest, EBSCO and more.

Deadline: see web site

Notification: see web site

Revision: see web site

Publication: see web site

Context-aware systems
Networking technologies
Security in network, systems, and applications
Evolutionary computation
Industrial systems
Evolutionary computation
Autonomic and autonomous systems
Bio-technologies
Knowledge data systems
Mobile and distance education
Intelligent techniques, logics and systems
Knowledge processing
Information technologies
Internet and web technologies, IoT
Digital information processing
Cognitive science and knowledge

Agent-based systems
Mobility and multimedia systems
Systems performance
Networking and telecommunications
Software development and deployment
Knowledge virtualization
Systems and networks on the chip
Knowledge for global defense
Information Systems [IS]
IPv6 Today - Technology and deployment
Modeling
Software Engineering
Optimization
Complexity
Natural Language Processing
Speech Synthesis
Data Mining

For more topics, please see web site <https://sites.google.com/site/ijcsis/>



For more information, please visit the journal website (<https://sites.google.com/site/ijcsis/>)

Editorial

Message from Editorial Board

*It is our great pleasure to present the **May 2019 issue** (Volume 17 Number 5) of the **International Journal of Computer Science and Information Security (IJCSIS)**. High quality research, survey & review articles are proposed from experts in the field, promoting insight and understanding of the state of the art, and trends in computer science and technology. It especially provides a platform for high-caliber academics, practitioners and PhD/Doctoral graduates to publish completed work and latest research outcomes. According to Google Scholar, up to now papers published in IJCSIS have been cited over **13299** times and this journal is experiencing steady and healthy growth. Google statistics shows that IJCSIS has established the first step to be an international and prestigious journal in the field of Computer Science and Information Security. There have been many improvements to the processing of papers; we have also witnessed a significant growth in interest through a higher number of submissions as well as through the breadth and quality of those submissions. IJCSIS is indexed in major academic/scientific databases and important repositories, such as: Google Scholar, Thomson Reuters, ArXiv, CiteSeerX, Cornell's University Library, Ei Compendex, ISI Scopus, DBLP, DOAJ, ProQuest, ResearchGate, LinkedIn, Academia.edu and EBSCO among others.*

A great journal cannot be made great without a dedicated editorial team of editors and reviewers. On behalf of IJCSIS community and the sponsors, we congratulate the authors and thank the reviewers for their outstanding efforts to review and recommend high quality papers for publication. In particular, we would like to thank the international academia and researchers for continued support by citing papers published in IJCSIS. Without their sustained and unselfish commitments, IJCSIS would not have achieved its current premier status, making sure we deliver high-quality content to our readers in a timely fashion.

"We support researchers to succeed by providing high visibility & impact value, prestige and excellence in research publication." We would like to thank you, the authors and readers, the content providers and consumers, who have made this journal the best possible.

For further questions or other suggestions please do not hesitate to contact us at ijcsiseditor@gmail.com.

*A complete list of journals can be found at:
<http://sites.google.com/site/ijcsis/>*

IJCSIS Vol. 17, No. 5, May 2019 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):



Open Access This Journal is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source.



Bibliographic Information

ISSN: 1947-5500

Monthly publication (Regular Special Issues)
Commenced Publication since May 2009

Editorial / Paper Submissions:

IJCSIS Managing Editor

ijcsiseditor@gmail.com

Pennsylvania, USA

Tel: +1 412 390 5159

IJCSIS EDITORIAL BOARD

IJCSIS Editorial Board	IJCSIS Guest Editors / Associate Editors
Dr. Shimon K. Modi [Profile] Director of Research BSPA Labs, Purdue University, USA	Dr Riktesh Srivastava [Profile] Associate Professor, Information Systems, Skyline University College, Sharjah, PO 1797, UAE
Professor Ying Yang, PhD. [Profile] Computer Science Department, Yale University, USA	Dr. Jianguo Ding [Profile] Norwegian University of Science and Technology (NTNU), Norway
Professor Hamid Reza Naji, PhD. [Profile] Department of Computer Engineering, Shahid Beheshti University, Tehran, Iran	Dr. Naseer Alquraishi [Profile] University of Wasit, Iraq
Professor Yong Li, PhD. [Profile] School of Electronic and Information Engineering, Beijing Jiaotong University, P. R. China	Dr. Kai Cong [Profile] Intel Corporation, & Computer Science Department, Portland State University, USA
Professor Mokhtar Beldjehem, PhD. [Profile] Sainte-Anne University, Halifax, NS, Canada	Dr. Omar A. Alzubi [Profile] Al-Balqa Applied University (BAU), Jordan
Professor Yousef Farhaoui, PhD. Department of Computer Science, Moulay Ismail University, Morocco	Dr. Jorge A. Ruiz-Vanoye [Profile] Universidad Autónoma del Estado de Morelos, Mexico
Dr. Alex Pappachen James [Profile] Queensland Micro-nanotechnology center, Griffith University, Australia	Prof. Ning Xu, Wuhan University of Technology, China
Professor Sanjay Jasola [Profile] Gautam Buddha University	Dr . Bilal Alatas [Profile] Department of Software Engineering, Firat University, Turkey
Dr. Siddhivinayak Kulkarni [Profile] University of Ballarat, Ballarat, Victoria, Australia	Dr. Ioannis V. Koskosas, University of Western Macedonia, Greece
Dr. Reza Ebrahimi Atani [Profile] University of Guilan, Iran	Dr Venu Kuthadi [Profile] University of Johannesburg, Johannesburg, RSA
Dr. Dong Zhang [Profile] University of Central Florida, USA	Dr. Zhihan Iv [Profile] Chinese Academy of Science, China
Dr. Vahid Esmaealzadeh [Profile] Iran University of Science and Technology	Prof. Ghulam Qasim [Profile] University of Engineering and Technology, Peshawar, Pakistan
Dr. Jiliang Zhang [Profile] Northeastern University, China	Prof. Dr. Maqbool Uddin Shaikh [Profile] Preston University, Islamabad, Pakistan
Dr. Jacek M. Czerniak [Profile] Casimir the Great University in Bydgoszcz, Poland	Dr. Musa Peker [Profile] Faculty of Technology, Mugla Sitki Kocman University, Turkey
Dr. Binh P. Nguyen [Profile] National University of Singapore	Dr. Wencan Luo [Profile] University of Pittsburgh, US
Professor Seifeidne Kadry [Profile] American University of the Middle East, Kuwait	Dr. Ijaz Ali Shoukat [Profile] King Saud University, Saudi Arabia
Dr. Riccardo Colella [Profile] University of Salento, Italy	Dr. Yilun Shang [Profile] Tongji University, Shanghai, China
Dr. Sedat Akleylek [Profile] Ondokuz Mayıs University, Turkey	Dr. Sachin Kumar [Profile] Indian Institute of Technology (IIT) Roorkee

Dr Basit Shahzad [Profile] King Saud University, Riyadh - Saudi Arabia	Dr. Mohd. Muntjir [Profile] Taif University Kingdom of Saudi Arabia
Dr. Sherzod Turaev [Profile] International Islamic University Malaysia	Dr. Bohui Wang [Profile] School of Aerospace Science and Technology, Xidian University, P. R. China
Dr. Kelvin LO M. F. [Profile] The Hong Kong Polytechnic University, Hong Kong	

TABLE OF CONTENTS

1. PaperID 30041902: Implementation of a Decision System for a Suitable IT Governance Framework (pp. 1-7)

Ibrahim HAMZANE, Information Technology and Modelization Lab (LTIM), Hassan II University Mohammedia, Casablanca, Morocco
Abdessamad BELANGOUR, Information Technology and Modelization Lab (LTIM), Hassan II University Mohammedia, Casablanca, Morocco

Full Text: PDF [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [ProQuest](#)]

2. PaperID 30041903: Palm Vein Feature Extraction Method by Using Optimized DVHLocal Binary Pattern (pp. 8-12)

Dini Fronitasari, Basari & Dadang Gunawan
Department of Electrical of Engineering, Universitas Indonesia, Depok, Indonesia

Full Text: PDF [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [ProQuest](#)]

3. PaperID 30041904: A Novel Framework to Improve Secure Digital Library at Cloud Environment (pp. 13-22)

Heba Sayed, Hesham N. Elmahdy, Fathy Amer, Sherif Shaheen
Faculty of Computers and Artificial Intelligence, Faculty of Arts, Cairo, University

Full Text: PDF [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [ProQuest](#)]

4. PaperID 30041905: Botnet Detection and Prevention in Software Defined Networks (SDN) using DNS Protocol (pp. 23-65)

Muhammad Junaid Zafar, Riphah International University, Islamabad, Pakistan
Professor Dr. Muhammad Zubair, Riphah International University, Islamabad, Pakistan

Full Text: PDF [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [ProQuest](#)]

5. PaperID 30041906: An Improved Approach for Monitoring and Controlling of Flyovers and Bridges Using Internet of Things (pp. 66-70)

K. S. F. Azam, D. M. Abdullah, Md. M. Rahman, Md. S. Bari
Department of Computer Science & Engineering, Primeasia University, Dhaka, Bangladesh

Full Text: PDF [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [ProQuest](#)]

6. PaperID 30041907: QoS Based Scheduling Techniques in Cloud Computing: Systematic Review (pp. 71-88)

Monika, Om Prakash Sangwan,
Guru Jambheshwar University of Science & Technology, Hisar, Haryana

Full Text: [PDF](#) [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [ProQuest](#)]

7. PaperID 30041910: Selecting Prominent API Calls and Labeling Malicious Samples for Effective Malware Family Classification (pp. 89-105)

Cho Cho San & Mie Mie Su Thwin

Cyber Security Research Lab, University of Computer Studies, Yangon, Myanmar

Full Text: [PDF](#) [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [ProQuest](#)]

8. PaperID 30041917: Text Extraction System by Eliminating Non-Text Regions (pp. 106-111)

S. Shiyamala & S. Suganya,

Department of Computer Science, Rathnavel Subramaniam College of Arts and Science, Coimbatore, TN, India

Full Text: [PDF](#) [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [ProQuest](#)]

9. PaperID 30041925: Optimizing Bigdata Processing by using Hybrid Hierarchically Distributed Data Matrix (pp. 112-124)

K. L. S. Soujanya (a), B. Shirisha (b), Challa Madhavi Latha (c)

(a) Professor, Department of CSE, CMR College of Engineering & Technology, Hyderabad, India.

(b) M.Tech Student, Department of CSE, CMR College of Engineering & Technology, Hyderabad, India.

(c) Assistant Professor, Department of Information Technology, Faculty of Informatics, University of Gondar, Gondar, Ethiopia

Full Text: [PDF](#) [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [ProQuest](#)]

10. PaperID 30041942: Design and Analysis of M-Shape Microstrip Patch Antenna for Wireless Communications (pp. 125-129)

Muhammad Afsar Uddin, Department of Computer Science & Engineering, Z.H. Sikder University of Science & Technology, Shariatpur, Bangladesh

Fatama Akter, Department of Computer Science & Engineering, Z.H. Sikder University of Science & Technology, Shariatpur, Bangladesh

Md. Zahid Hossain, Assistant Maintenance Engineer (Hardware) Dhaka WASA, Dhaka, Bangladesh

Full Text: [PDF](#) [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [ProQuest](#)]

11. PaperID 30041943: Children Cognitive Load Analysis in Affordance-based Interaction (pp. 130-134)

Syed Asim Ali, Department of Computer Science, University of Karachi, Pakistan -75270, Pakistan

Areeba Hafeez, Institute of Business Administration, Computer Science, Karachi-74400, Pakistan

Shereen Akram, Institute of Business Administration, Computer Science, Karachi -74400, Pakistan

Muhammad Affan Khan, Institute of Business Administration, Computer Science, Karachi -74400, Pakistan

Afshan Ejaz, Institute of Business Administration, Computer Science, Karachi -74400, Pakistan

Full Text: [PDF](#) [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [ProQuest](#)]

Implementation of a decision system for a suitable IT governance framework

Ibrahim HAMZANE

Laboratory of Information Technologies and Modeling
Hassan II University Mohammedia,
Casablanca, Morocco
hamzane.ibrahim@gmail.com

Abdessamad BELANGOUR

Laboratory of Information Technologies and Modeling
Hassan II University Mohammedia,
Casablanca, Morocco
belangour@gmail.com

Abstract— The implementation of IT governance is important to lead and evolve the information system in agreement with stakeholders. This requirement is seriously amplified at the time of digital area considering all the new technologies that has been launched recently (Big DATA, Artificial Intelligence, Machine Learning, Deep learning...). Thus, without a good rudder, every company risks getting lost in a sea endless and unreachable goals.

This paper aims to provide decision-making system that allow professionals to choose IT governance framework suitable to desired criteria and their importance based on a multi-criteria analysis method (WSM), we did implement a case study based on our analysis in a Moroccan company. Moreover, we present better understanding of IT Governance aspects such as standards and best practices.

Our article goes into a global objective that aims to build an integrated generated meta-model for better approach of IT Governance.

Keywords—component; IT Governance; COBIT; ISO 38500; CMMI; ITIL; TOGAF; PMBOK; PRINCE 2; SCRUM

I. INTRODUCTION

Information Technology is a business asset that is gaining a lot of importance in the last decades on every industry especially regarding the spread of new technologies.

Following the statistics provided by CIGREF in 2017, 51% of companies rely on COBIT for the governance of their information systems (IT), while 16% use internal processes and 32% are not inspired by COBIT in the world [22]. In Morocco, we have to make lot of effort regarding IT governance [20].

Our goal is to provide the most complete IT governance approach based on existing models and complement our research with other best practices in several IT domains. In this paper, we will clarify the difference between several concepts similar to the definition of the standards. Then, we will carry out a comparative study between the different frameworks specifying their strengths and weaknesses then we will implement a decision system based on our analysis that we will use on a Moroccan company. Thus, companies can weigh the

criteria and produce the choice of reference to adopt based on their own needs.

II. STANDARDS VS BEST PRACTICES

Outside, when we focus on governance practices specifically in IT governance, we come across several sources (ITIL, CNIL, SOX, CMMI, ISO 9001, ISO 9002, ISO 14000, ISO 17799, ISO 27001, 27002, 27003, 27005...) each reference offer a partial view of IT Governance. Thus, for better governance of our paper, we will first make a vocabulary distinction between theses references then we will define IT governance.

A. Standards

According to ISO and IEC: the standard is "a document established by consensus and approved by a recognized body, which provides, for common and repeated use, rules, guidelines or features, for activities or results that guarantee an optimal level of order in a given context." [1].

- ISO 38500: Helps business leaders to ensure that the use of IT assets positively and contributes to the performance of the organization by meeting the requirements of ISO / IEC 38500, organizations are able to monitor the use of IT, ensure business continuity and sustainability, align IT assets to business needs and ensure proper implementation and operation of IT assets [16].
- ISO 9001: Standard that establishes the requirements for a quality management system. It helps businesses and organizations become more efficient and increase customer satisfaction [20].

B. Best Practices

Whereas best practices are a set of behaviours to adopt and adapt to effectively manage a given aspect of IT such as : governance, value and quality of services, projects, processes, application development, development architecture, etc. Each IT aspect is considered essential by most professionals in the field, it can be found in the form of guides to good practice

such as SCRUM or adopted by organization such as PRINCE 2 (OGC), ITIL (OGC) or COBIT (ISACA).

Best practices are generally based on two types of models:

- Stepped models: structured by maturity levels; For example: CMMI, eSCM-CL ...
- "Continuous" or "Cyclical" models: structured by skill or phase domain; for example: ITIL 2011, TOGAF 9.2, COBIT 5 ...

Note that CMMI proposes both approaches.

Below some definitions of most commune best practices used in IT services.

- CMMI: Capacity Maturity Model Integrated is a model for assessing the maturity level of a company in terms of IT developments. Developed in 1987 by the Carnegie Mellon University Software Engineering Institute, CMMI is a model for the development and maintenance of computer systems and applications designed to capture, evaluate and improve the operations of engineering firms [3].
- COBIT: A framework for the development, implementation, supervision and improvement of the governance and administration practices of information systems. The IT Governance Institute and ISACA publish the COBIT framework. Its purpose is to provide a common language for business leaders to discuss together their goals, objectives and results [16].
- TOGAF: The Open Group Architecture Framework is a set of concepts and an industry standard covering the field of enterprise IT architectures [17].
- ITIL: Information Technology Infrastructure Library, is a framework enables information technology (IT) to play a service delivery role rather than just specialized support [11...14]. ITIL guidelines and best practices aim to adapt IT actions and budget to business needs and modify them as the company grows or changes direction. The goal is to improve efficiency and achieve predictable levels of service [9].
- PMBOK: Project Management Body of Knowledge is a project management guide designed and produced by the PMI Project Management Institute. This extensive guide aims to stabilize and structure the current knowledge needed to run a project in the best conditions.
- PRINCE 2: Projects In Controlled Environment is a method developed by the British government and accredited by Axelos, based on best practices in project management. This flexible methodology applies to all companies and only for a defined scope project. "Built upon seven principles, themes and processes, PRINCE2 can be tailored to meet specific requirements". [19]

- SCRUM: An agile project management methodology, it is used particularly in software development. It's "a framework within which people can address complex adaptive problems, while productively and creatively delivering products of the highest possible value." [18]

III. IT GOVERNANCE

Governance is the set of processes that tend to harmonize the world of business, projects and experience.

According to the CIGREF, governance is closely linked to the notion of company management.

IT governance [2]: "Organizational capacity exercised by the management committee, senior management and IS managers to oversee the formulation and implementation of the IS strategy".

The ITGI provides business executives and boards of directors with original research, online resources and case studies to help them meet their responsibilities in the area of IT governance.

It designed and authored COBIT V4.1, essentially as a teaching resource for information managers, general management, Information System management and control professionals [5].

Today, IT governance as defined by ITGI and ISACA boils down to the following 5 issues:

- IT Strategic Alignment
- IT Value Delivery
- IT Risk Management
- Performance Measurement
- IT Resource Management

According to the ISO, there are six guiding principles for corporate governance that apply to most organizations. The ISO specifies that each principle refer to what should exist, but does not describe how, when or by whom these principles were implemented. Nevertheless, decision-makers must demand that these principles be applied:

- Principle 1: Responsibility
- Principle 2: Strategy
- Principle 3: Acquisition
- Principle 4: Performance
- Principle 5: Compliance
- Principle 6: Ethics

IV. COMPARATIVE STUDY OF IT GOVERNANCE REFERENCES

A. Mini SWOT Analysis

In this section, we present a minimal SWOT analysis in order to summarize the strengths and weaknesses of the references:

TABLE I. SWOT ANALYSIS MINIMAL

CMMI	
Positives	Improve the quality of the product delivered and the productivity of the project
	Increase customer satisfaction by better meeting its requirements
	Reduce costs and meet deadlines
	Give better visibility to management and enable better risk management
Negatives	The lack of precision
	The level of maturity being global, it can mask areas of the organization that perform less well than others perform and hide gaps in certain process areas
COBIT	
Positives	Meeting the needs of stakeholders
	Cover the entire company from end to end
	Application of a single Framework
	Provide a holistic approach to business decision-making
	Separating the governance from the management
Negatives	Difficulty of implementation
	Management guide not known in the framework
TOGAF	
Positives	A common language within the company
	Strength of the information system (as growing complexity of IS)
	Maximize IT value
	Use a common framework to facilitate the search for skills
	Achieve better quality of products
	Does not cover management processes
Negatives	Does not cover management processes
	Does not cover support services, the build and implementation services
ISO 38500	
Positives	Assuring all stakeholders (including customers, shareholders and employees) that if the standard is applied, they can trust the IT governance of their organization
	Informing and guiding leaders to steer the use of computers in their organization
	Providing a framework for an objective assessment of the company's IT governance
Negatives	Framework designed for top management.
	Does not cover support services, the build and implementation services
ITIL	
Positives	Time saving
	Cost reduction
	Defining more precise roles and responsibilities
	Better user satisfaction
	Better productivity / efficiency
	IT services of better quality
Negatives	Adaptation to customer needs facilitated
	Very little known to the general public
	There is very little information on the Internet

CMMI	
ITIL	
Complex (you have to be expert as it concerns the network, system, application, BD and have a global vision of the IS)	
PMBOK	
Positives	A guide to knowledge and good practice created by project management professionals who update it regularly.
	Standardize project management practices, which means that each department works in the same way.
	Find the same practices from one company to another.
Negatives	Respect all PMBOK processes to ensure the success of the project
	Adapt the methodology to the size and sector of the project
PRINCE 2	
Positives	Rational project management.
	The formalism makes it possible to define a logic and a common vocabulary facilitating exchanges
	Continuous learning orientation
Negatives	Systematic rationalization disguises the real subtleties of project management, in practice; project management is much more complex. The realities of the field, the human stakes, the immature technologies, the requirements of deadlines and budgets will not be solved by the obsession of the formalism
SCRUM	
Negatives	Increase the fluidity of release and velocity of the team
	Easily master the risks and changes during delivery
	Encourage orientation, rigor and energy in the teams
	Increase the capacity and quality of execution relative to customer requirements
	Substantially outperform the delivery of priority values that generate results faster
Negatives	Requires a united and motivated team
	Difficulty following the life cycle of a development
	Support needed by sponsors
	Essential adaptation phase (continuous changes)

B. Multi-criteria comparative study

1) Multi-criteria analysis

After seeing the advantages and disadvantages of each framework, we will now develop a multi-criteria analysis between these frameworks. A Multi-Criteria Decision Analysis, or MCDA, is a valuable tool that can be applied to many complex decisions. It can solve complex problems that include qualitative and/or quantitative aspects in a decision-making process.

We aim to help the decision-makers by facilitating the choice of the best framework to use according to desired criteria and their importance.

The score of a framework is calculated based on a number of criteria. So far we have identified ten criteria; Indeed, thus, based on the set of principles of IT governance for the ITGI and ISO 38500, we have identified in almost complete governance pillar that will be our important criteria: IT Strategic Alignment, IT Value Delivery, IT Risk Management,

IT Performance measurement, IT Acquisition, IT Resource Management, IT Responsibility, IT Compliance, IT Human Behaviour and IT Control.

- C1: IT Strategic Alignment: An approach to align the information system strategy with the company's business strategy.
- C2: IT Value Delivery: Value creation refers to the financial purpose of companies for their IT. Value is created when investments are based on IT whose rate of return is higher than the costs that are made.
- C3: IT Risk Management: Operational and business risk in relation to IT, it is about setting up processes to manage IT risk.
- C4: IT Performance measurement: The implementation of KPIs to achieve the objectives. In addition to the indicators, it is also the right definition of the objectives to be put in place.
- C5: IT Acquisition: The management of the service providers and the external interventions makes it possible to carry out the objectives of the IT thus a good piloting of the activity IT.
- C6: IT Resource Management: The main asset of the IT division is the human re-sources as well as the materials used, thus a good management of the re-sources makes it possible to obtain good governance of the IT system.
- C7: IT Responsibility: The definition of roles and responsibility is a key factor of process success so it is a pillar to carry out the adopted processes.
- C8: IT Compliance: IT regulation has evolved a lot in the last decades, with user protection laws, a good benchmark allowing a good application of IT regulations will allow better governance.
- C9: IT Human Behavior: According to the CNIL, the respect of the freedom is an important axis for a good IT governance; several articles describe in detail this pillar.
- C10: IT Control: Set up a set of business processes / IT with KPIs to control the execution and performance of processes.

2) Multi-criteria analysis methods

There are several possible methods to make the comparison between the frameworks using a number of criteria. These methods can be divided into three main families:

- Complete aggregation (top-down approach): Aggregating the n criteria to reduce them to a single criterion.
- Partial aggregation (bottom-up approach): Comparing potential actions or rankings to each other, and establishing between them outranking relations.

- Local and iterative aggregation: Looking primarily for a starting solution, then, we proceed to an iterative search to find a better solution.

The table 2 shows the different existing multi-criteria methods sorted by family:

TABLE II. MULTI-CRITERIA ANALYSIS FAMILIES [17]

Family	Approach	Methods
Complete aggregation	top-down approach	Weighted Sum Method (WSM) TWO WAY ANOVA Weight Product Method (WPM) Analytic Hierarchy Process (AHP) Multi Attribute Utility Theory (MAUT)
Partial aggregation	bottom-up approach	ELECTRE Promethe Melchior Qualifex Oreste Regim ...
Local and iterative aggregation	Local & iterative	Improving Cones Method (ICM) GOAL Programming STEM Branch and Bound

3) Weighted Sum Method (WSM)

We chose the Weight Sum Method (WSM) for our analysis. Indeed, this method allows us to find the best possible approach by assigning a weight to each comparison criterion, it allows to take into account all the criteria according to their value and without a criterion penalizing the other criteria.

4) Comparison criteria and weight

We presented the ten comparison criterions cited on which the comparative study will be based. We notice that these criteria are based on the characteristics of each of the approaches presented in the comparative study and the SWOT analysis presented above, we summarized all the characteristics (strengths and weaknesses) in ten global criteria to ensure better analysis and optimize the comparison.

These criteria have the same importance, therefore the WSM weight will be the same for each criterion and equal to "1". However as we will see further in this paper the weight of each criterion will change depending on each company. We will present a case study on which we will expose the vision of a reel company weighs.

5) Comparison criteria and weight

The WSM method start with filling the multi-criteria choice matrix. The columns contain the frameworks to be compared and its lines contain criteria with the weight assigned to each criterion witch we agree that it's "1" as all the criterions have the same importance, and in cells there is the score given to each framework based on the detailed comparative study of each framework [2] [3] [5].

About the score, we will then use the maturity model, which consists of five levels of maturity to weight the criterion

on each framework, each level will give a score, for example “level 1” will leave a score of “1”.

We recall the definition of the 5 levels by modifying the definitions to apply it to our case:

- **Level 1:** There is no formal method, nor coherence, nor standard, based on which the criteria will be constructed. The development process of the criteria is not described formally in the framework.
- **Level 2:** There is a consensus in the framework of how the criteria should be managed, but this has not been formalized or described.
- **Level 3:** The development process of the criteria is formalized, documented and applied. Reviews are conducted with compliance and the configurations are properly managed.
- **Level 4:** The reference has instituted a formal metric information collection process to track and manage the criteria development process as well as the resulting systems. Indicators monitor the smooth running of processes and the respect of the quality objectives of the criteria.
- **Level 5:** The reference uses measures to continuously optimize the criteria development process. It describes in detail a process of correcting the aspects that would be considered insufficient by reading the indicators allowing manage the criteria.

The Table 3 bellow represents the resulting multi-criteria choice matrix according to the score of each criterion:

TABLE III. MULTI-CRITERIA CHOICE MATRIX

	CMMI	COBIT	TOGAF	ISO 38500	ITIL	PMBOK	PRINCE 2	SCRUM
C1	4	4	3	3	3	1	3	3
C2	3	4	4	4	4	3	3	3
C3	3	4	4	2	3	5	5	4
C4	4	5	3	4	3	4	4	4
C5	1	2	2	1	1	1	1	1
C6	1	1	2	1	2	4	2	2
C7	4	3	1	3	1	1	1	1
C8	3	2	2	1	1	1	1	1
C9	3	3	3	3	3	2	2	2
C10	4	4	2	2	3	1	5	1

We convert the table into a spider chart for visual purpose; we notice that there is no complete reference; however, COBIT is the most complete according to our investigations, see Fig. 1.

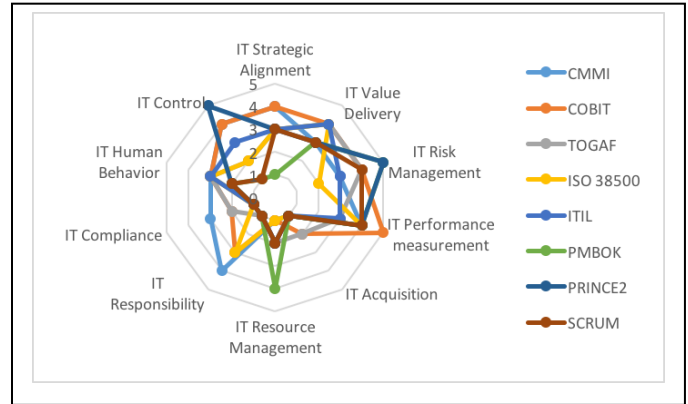


Figure 1. Spider chart Multi-Criteria Decision

6) Discussion

The components of good governance are not applicable on all the reference systems.

As we analyse the results, we find that CMMI covers 62% of the components of the IT governance whereas COBIT covers 65% of the foundations of a good governance, on the other hand PMBOK presents the least percentage of application with only a rate of 43% which is normal since it does not contain a methodology but it is a set of practice project in management grouped in a reference.

We will scan the components and dissect the key values of each of the components, indicating which repositories apply them best.

We found that COBIT and CMMI respond best to strategic alignment given their commitment to corporate values with a clear definition of the processes, so they allow a comprehensible vision by the management of what is done by the company. Due to the process approach and compliance, a clear attribution of ownership and responsibilities deal with the requirements for control of the IT environment.

Value creation is present on almost all repositories because it is the essence of the implementation of IT in the company whatever the chosen repository.

Risk management is an important component of IT governance; it allows identifying risks in a clear and structured way. With a clear knowledge of all the risks a company is exposed to, it can prioritize them and take the appropriate measures to reduce losses and reduce the total cost of risk, most of the standards are based at least on strategies of risk management according to the intervention layer, whether operational or organizational.

IT governance processes are evaluated, directed and controlled. Indicators are a monitoring mechanism helping the achievement of business and IT objectives.

As a result, there is no complete repository of IT governance, however the most complete reference is COBIT given the positions it takes on each of the components.

V. CASE STUDY

We consulted the company USA HOME; a company specialized in cameras installation, maintenance of pointing software, and office installation. Given the competition in the Moroccan market, the CEO want to optimize the IT resources and apply an IT Governance to it's IT department.

Based on our study we build up an application form in order to get the interests of the company on every criterion, below the result given by the CEO of USA HOME (Fig 2):

Figure 2. Application form that was given to the company USA HOME

Following the input of the CEO, the Multi-Criteria Choice Matrix has changed through the formula (1) below:

$$(5 * A * B) / X = Z. \quad (1)$$

- Z New score following the preferences of the company
- B Initial score produced
- A Weight according to the company
- X Sum of weights regarding all the criterions

As a result, Spider chart Multi-Criteria Decision has changed according to the company's need (Fig 3):

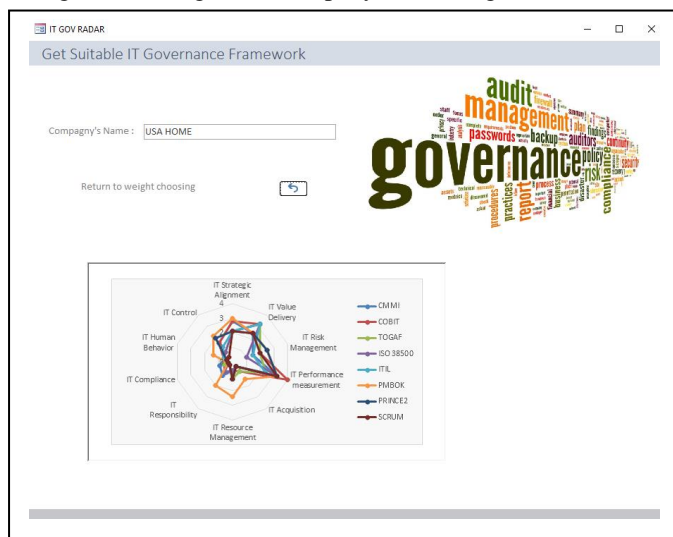


Figure 3. Spider chart Multi-Criteria Decision of USA HOME

According to our Multi-Criteria Decision form, PMBOK will be a good reference based on the company USA HOME requirements. It will allow the company to enhance the potential of creativity, ensuring the realization and coordination of project actors and available resources according to the defined plan; it's also an effective way for a company very concerned by the projects.

VI. CONCLUSION

IT assets has become directly linked to the results of the business; as the launch of new technologies and the digitalization of companies in all domains. Thus, the implementation of IT governance is important to lead and evolve the information system in agreement with stakeholders.

The choice of an IT governance framework is very important task before the implementation, a good choice will lead to better result, this article has enabled us to implement a decision system according to the company needs. Also, to understand IT governance framework regarding their advantages and disadvantages.

We have seen that all frameworks have many challenges specially in covering all business areas and the difficulty of implementation. As future work, we will present solutions for these issues. This work gives a contribution for professionals to help them choose between different existing framework, and this according to their needs and criteria that matter most to them, as we have seen in the case study.

REFERENCES

- [1] Alexandre Steigmeier, Rolf Hauri, Gouvernance de la sécurité : comment articuler les différentes normes et méthodes, Novembre 2009.
- [2] The National Computing Center, developing a succesful governance strategy, Novembre 2005.
- [3] Jarke, M. Mylopoulos, J. Schmidt, and Vassilou Y. DAIDA, Conceptual Model-ing and Knowledge Based Suppor of Information Systems Development Process. Technique et Science Informatiques, 1990, 122-133.
- [4] Jean-François CARPENTIER, La gouvernance du Système d'Information dans les PME : Pratiques et évolutions, Editions ENI, Mars 2017.
- [5] Bruno Ménard, CobiT : Pour une meilleure gouvernance des systèmes d'information, Eyrolles, janvier 2009.
- [6] Frédéric Georgel, IT Gouvernance : Maîtrise d'un système d'information, Dunod, Mai 2005.
- [7] Richard Basque, CMMI 1.3 - Guide complet de CMMI-DEV et traduction de toutes les pratiques CMMI-ACQ et CMMI-SVC, Dunod, Mai 2011.
- [8] Gmati, I., Nurcan, S., Gmati, I., & Nurcan, S. Un cadre de référence pour analyser les exigences d'alignement métier / système d'information, 2012.
- [9] Abbadi, S. S.-M.-L. Proposition de méthode d'implémentation d'ITIL. 2eme édition du congre International de génie Industriel et Management des systèmes, 2015, Mai 21, pp. 5,6.
- [10] Rolland, C.. A Comprehensive View of Process Engineering, 2012, 1-24.
- [11] Commerce, O. o. ITIL 2011 Amélioration continue des services. stationery office, 2011.

- [12] Commerce, O. o. ITIL 2011 Conception des services, stationery office. stationery office, 2011.
- [13] Commerce, O. o. ITIL 2011 Exploitation des services. stationery office, 2011.
- [14] Commerce, O. o. ITIL 2011 Stratégie des services. stationery office, 2011.
- [15] Commerce, O. o. ITIL 2011 Transition des services. stationery office, 2011.
- [16] Martine Otter, J. S. Guide des certifications SI. Dunod, 2009.
- [17] Z. Ibn Batouta, Multi-criteria analysis and advanced comparative study between automatic generation approaches in software engineering, 2015. Vol.81. No.3
- [18] Ken Schwaber, Jeff Sutherland, "The Definitive Guide to Scrum: The Roles of the Game", 2017 Edition, available at www.scrum.org
- [19] AXELOS, "Managing Successful Projects with PRINCE2", 2017 Edition
- [20] H. Askari, H.Mohammad khan, L. Mydin, "Reformation and Development in the Muslim World: Islamicity Indices as Benchmark", Springer 2017 Edition
- [21] R. Tricker, "ISO 9001:2015 for Small Businesses", 2016 Edition
- [22] CIGREF, "Les référentiels de la DSI", www.cigref.fr

Palm Vein Feature Extraction Method by Using Optimized DVHLocal Binary Pattern

Dini Fronitasari¹, Basari² and Dadang Gunawan³

Department of Electrical Engineering

Universitas Indonesia

Depok, Indonesia

dini.fronitasari61@ui.ac.id

Abstract— Intrinsic biometric, nowadays, has become a trend in research on human identification due to some disadvantages of the extrinsic biometric features. Extrinsic biometric features are easily imitated and lost as they are located outside the human body and are easy to change due to accidents. Therefore, in this paper we focus on a method which can extract a feature from an image of intrinsic biometric. Moreover, we use palm skin vein as the intrinsic biometric feature for human recognition application. The feature of an image can be extracted by using a specific method, such as Local binary pattern (LBP), which has been commonly used in many research works. A modified LBP, called cross-LBP (DVHLBP), has been proposed in our previous paper. DVHLBP has better performance compared with the conventional LBP. In this paper, we further optimize the DVHLBP method. In this paper, DVHLBP is used as the extraction feature algorithm on palm vein and histogram intersection is used for the matching process. In the simulation, the ratio of data model to data testing was 5:5. Testing was done by applying some scenarios. The optimization is done by examining the number of regions that yield the optimal threshold value. The optimal configuration is achieved when we use 8 neighborhood pixels with radius of 12, 16 regions. Simulation results show that the false accepted rate (FAR) and false rejected rate (FRR) are 0.01 and 0.01, respectively, with recognition rate of 99%. In addition, we show that the optimized DVHLBP has improvement in the accuracy and equal error rate (EER).

Keywords— *Biometric, palm vein recognition, pattern recognition, local binary pattern (LBP), diagonal vertical horizontal local binary pattern (DVHLBP), KNN.*

I. INTRODUCTION

A biometric systems, recently, has become more reliable in as recognition system, in which the physical and behavioral characteristics of an individual are made to be the unique features. One of the unique features commonly used as the biometric feature is the palm vein.

A palm vein is popular for its special structure pattern as the representation of an individual. A palm vein is the intrinsic feature of an individual which has more benefits than other features, e.g. it is difficult to be forged because it lies under the skin, it is uncorrupted, and it cannot be used for a dead individual. We cannot use an ordinary camera or bare eyes to capture a palm vein image. Instead, a special near infrared (NIR) camera is required [1].

Biologically, a vein is a part of body circulation that delivers blood from heart to other organs in the whole body

and vice versa. As mentioned before, a vein network at human's hand has its unique feature. Each individual has his/her own unique vein network pattern. This encourages many researchers to work on palm vein pattern, where the pattern is used as the input for a biometric system [3].

Research works on biometric system, especially palm vein, have been intensively explored by many researchers until today [2][3][4][5]. Hence, in this paper, we improve the performance of palm vein identification system by optimizing the cross local binary pattern (DVHLBP) algorithm. DVHLBP algorithm has been used as the feature extractor to improve the system performance. It has been shown in our previous work [10] that the DVHLBP method could achieve better performance than the method presented in [11]. The aim of this paper is to optimize the parameters of the DVHLBP.



Figure 1. Palm Vein Recognition

The rest of the paper is organized as follows. Section II discusses the palm vein image preprocessing technique. Section III presents the feature extraction by using DVHLBP algorithm. Section IV discusses the matching process by using the histogram intersection while the testing scenarios appear in Section V. Finally, Section VI provides the conclusion of this paper.

II. PREPROCESSING

In a biometric system, acquisition of an image with unique feature is essential. We use a specific part of a palm vein image, i.e. the middle part, to get an optimal feature extraction. Region of interest (ROI) of the palm image extracts the texture of the vein pattern and must be determined beforehand. Boundary line of the hand is selected before detecting the valley points. Valley points are used to construct the rectangular ROI containing the vein texture

pattern. The rectangular ROI is constructed by connecting the valley points. Figure 1 shows the image preprocessing diagram.

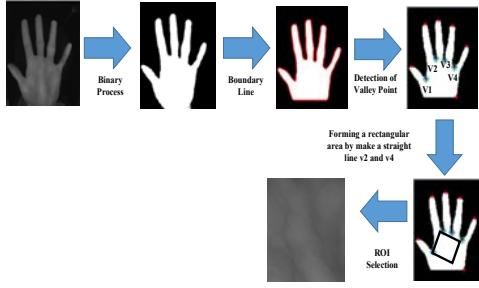


Figure 2. Preprocessing module.

After ROI selection, the next process is to equalize the palm vein image size. The equalization is necessary to avoid the varying size of the palm vein image due to the extraction feature process. We use 256 x 256 image size for simulations. The whole procedure for palm vein recognition process is depicted in Figure 2.

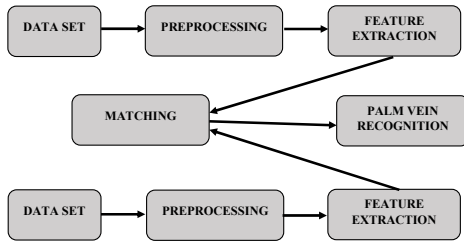


Figure 3. Recognition system.

III. FEATURE EXTRACTION USING DVHLBP

As previously mentioned, we focus on the feature extraction using DVHLBP method. This method is developed from the conventional LBP method. The DVHLBP is employed in a matrix of 3x3 accompanied by 8 neighborhood pixels and 1 center pixel which is placed in the center of the matrix. Figure 3 shows the description of the DVHLBP flowchart.

A. Build Index Tabel

The index table is the main domain to save the selected pixel value after DVHLBP process. DVHLBP provides a certain value after comparing the neighbors of a pixel. Then, the value is stored in the index table.

B. DVHLBP Method

DVHLBP is a method developed from LBP. The process is similar to LBP. We compare the value of a pixel with its neighborhood pixels resulting in a group of bits which is converted to decimal numbers. Figure 3 shows the process of DVHLBP.

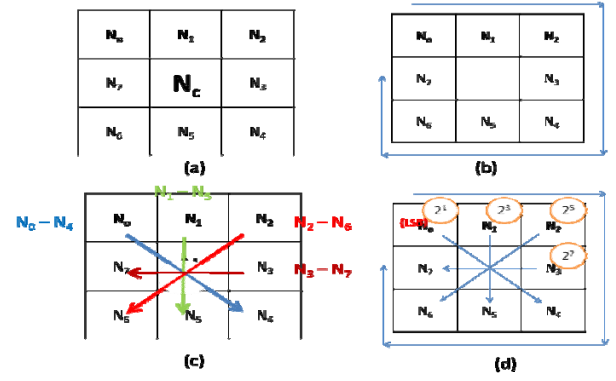


Figure 4. DVHLBP Method

$$DVH_LBP_{P,R}(x,y) = \sum_{k=0}^{P-1} \frac{1}{2} \left(\frac{N_k - N_c}{N_k - N_c} \right) 2^{2k+1} + N_c \quad (1)$$

The binary threshold function $S(\delta)$ is given as

$$S(\delta) = \begin{cases} 0, & \delta < 0 \\ 1, & \delta \geq 0 \end{cases}$$

DVHLBP using linear interpolation of the pixel values allows the choice of any radius (R) and a number of pixels in the neighborhood (P).

C. Region Cutting

Palm vein image is split into smaller parts as local features. Each part is extracted by LBP extraction and it takes histogram feature (as global feature) of the palm vein image. By splitting the image into smaller parts, the accuracy of the divided portion of the data model and data testing increases. The increase is caused by the matching process done in each region of the data model to each region of data testing. This concept has been applied in [3] where LBP Multi block concept was used for face recognition system yielding recognition rate up to 97%. The comparison of the similarity was better than 2 images testing through separated regions. In this research, we split 16 regions of a palm vein image before the feature extraction process.

D. Histogram Extraction

The results of DVHLBP process has been obtained at each region of palm vein image. Then, the feature of histogram is extracted. The histogram values are concatenated to become one feature. In this research, histogram value of 16 regions is extracted and collected to be one feature. The 16 regions of histogram are merged into one feature.

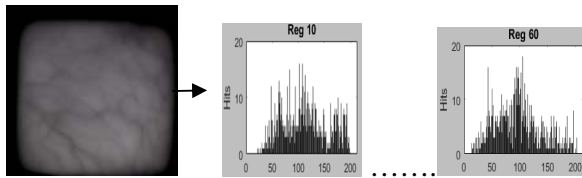


Figure 5. Histogram Extraction and Merging Histogram Feature.

IV. MATCHING

A. Similarity Measurement

Histogram intersection method is chosen to measure the similarity between two images for identification. The intersection of histogram provides higher value for identifying the performance, since no background and foreground are necessarily divided [7] [8].

$$H(p, q) = \frac{\sum_i \min(p_i, q_i)}{q_i} \quad (2)$$

The compared histograms are respectively represented by p and q , and i which is the binary of the histogram [6]. The result of histogram intersection is between 0 and 1. The higher the value, the closer it is to 1 and the higher the similarity of the two histograms.

B. Decision

The main problem of the research of palm vein recognition is whether the data testing is registered/accepted by the system or unregistered/rejected by the system. Acceptation/rejection is done by a threshold value which is determined before. If the result of matching is more than or equal to the threshold value, the data testing is accepted. If the result of matching is less than or equal to the threshold value, the data testing is rejected. The threshold value is determined by some calculations. Firstly, threshold array (TA) is obtained by calculating the histogram intersection of data model for each individual. Secondly, minimum and maximum values of TA are found out. Delta value can be obtained by this formula.

When the threshold is optimal, the system threshold is set by comparing the difference value of the false rejected rate (FRR) and false accepted rate (FAR) or the same as the rate of error on the intersection of FAR and FRR on the region of convergence (ROC) curve.

V. TESTING SCENARIO

In this simulations, some test scenarios are conducted to obtain optimal parameters and to examine the system performance in development. The system of biometric has two rudimentary forms of faults: FAR and FRR [5]. System performance analysis is performed with a measurement metric shown by the ROC curve. The performance is obtained from the intersection between The FRR and FAR curves denoted as (ERR) that stands for Equal Error Rate. Smaller ERR value results in higher performance.

A. Hardware and software specification.

The test run on a computer with an Intel (R) Core (TM) i5 3.1 GHz processor and 4 GB RAM using the Windows 7 64-bit operating system and MATLAB R2019a simulation tools.

B. Dataset

This study utilizes dataset of CASIA with multi-spectral palm print that consists of palm vein image of 850 nm (with 850 nm illuminator). The image contains 768 x 576 pixels that belong to individuals having ID 001 – 050 and 3 samples for each individual with label 01 – 03.

B. Performance Measurement

The performance measurement was using accuracy, and FAR and FRR. The accuracy is calculated by using:

$$\text{Accuracy} = \frac{\text{Number of Correct Pair}}{\text{Number of Test}} \times 100\% \quad (3)$$

While FAR and FRR were calculated using the formulae:

$$\text{FAR} = \frac{\text{False Acceptance}}{\text{Number of Test}} \quad (4)$$

$$\text{FRR} = \frac{\text{False Rejection}}{\text{Number of Test}} \quad (5)$$

We use four scenarios to test the palm vein recognition system as described in Table 1.

Table 1. Examining the scenario

Scenario	Description	Purpose
Scenario 1	Testing parameters P (neighboring) and R (radius) on DVHLBP method with ratio of model data and test data of 5:5, the palm vein image is divided into 16 regions.	This test is done to find the optimal P and R in the DVHLBP method by viewing the best accuracy generated.
Scenario 2	Testing the number of regions of a palm vein image, with the ratio of model data to test data of 5: 5, and the configuration in scenario 1. In this scenario, we test the accuracy of the result obtained with a number of varied regions.	The purpose of this test is to obtain the optimal number of regions by looking at the best accuracy obtained.
Scenario 3	Performing threshold value search to calculate the performance of FAR and FRR values from this biometrics system, with the ratio of model data to test data of 5:5, and the configuration in scenarios 1 and 2.	This test is aimed to obtain the optimal threshold value by finding the smallest difference between FAR and FRR, or FAR and FRR intersections on the ROC curve (equal error rate).
Scenario 4	Examining the variation of the palm vein image size adjustment, with the ratio of model data to test data of 5:5, and the configuration in scenarios 1, 2, and 5.	The purpose of this test is to examine the performance of the recognition rate on the shape of the change of image size of the processed palm vein.

VI. TESTING RESULT

A. Scenario Analysis 1

Table 2 shows the results of system accuracy with the changes in the parameter value tested. It can be seen that the optimum accuracy is obtained when $P = 8$ and $R = 12$.

Table 2. Scenario 1 Test Result

Parameter	Training Data	Testing Data	Accuracy (%)
P=8; R=1	150	150	92%
P=8; R=4	150	150	90%
P=8; R=6	150	150	94%
P=8; R=12	150	150	99%

Table 3. Scenario 1 Test Result

Parameter	Training Data	Testing Data	Accuracy (%)
P=16; R=1	150	150	85%
P=16; R=4	150	150	80%
P=16; R=6	150	150	88%
P=16; R=12	150	150	85%

Table 3 shows the results of accuracy measurements of the two tested parameters. It can be seen that at the number of neighbors of 16, we start the test at the number of radius of 4. This is because the number of radius smaller than 4 produces a poor performance due to the buildup point neighbors in the image pixel blocks and the unavailability of the pixel block area that holds 16 numbers of neighbors in the radius.

It is known that at the number of neighbors of 8, it produces the best accuracy of 99%. It has increased from our previous paper [10] by using the same extraction feature with the same parameter but different in the classification process. When the number of neighbors is 16, the system yields the best accuracy, which is 88.00%. Therefore, it can be seen that 16 is the optimum number of neighbors and 6 is the optimum radius. By examining that the best accuracy is obtained by the number of radius of 12, it can be concluded that 8 neighbors ($P = 8$) and radius of 12 ($R = 12$) are the optimal parameter for DVHLBP configuration.

B. Scenario Analysis 2

Table 4. Scenario 2 Test Result

No.	Number of Region	Training Data	Testing Data	Accuracy (%)
1	4	150	150	92%
2	16	150	150	99%
3	25	150	150	97%
4	64	100	150	96%
5	128	150	150	88%

Table 4 presents the results of the accuracy measurements on the number of regions tested. It can be seen that the best accuracy is 99 with 16 regions, while for the smaller number of regions, e.g. 4, it results in an accuracy of 92%, and for larger regions, e.g. 25, 64, and 128, it results in 97%, 96.00%, and 88% accuracy, respectively. It can be seen that the number of regions with the addition of the number of regions from 4 regions to 16 regions increases the accuracy but when we increase the number of regions from 16 regions to 25 and 64 regions, we have a decreasing accuracy. This is due to the increasing number of regions so that smaller image size will be processed which effect the complexity of the process of image matching. Therefore, 16 is the optimal number of regions which results in accuracy of 99%.

C. Scenario Analysis 3

Scenario 3 is done to examine the performance of the ERR by showing the point of intersection of FRR and FAR on ROC curve with the ratio of model data to test data of 3: 3, and configuration of best parameter in scenarios 1 and 2. FAR shows the acceptance error on the system where the test data not listed in the system are considered to be registered in the system. On the other hand, FRR is a refusal error on the system where the test data listed are considered not listed in the system. FAR and FRR are obtained by using a threshold value that determines the system acceptance and rejection decision. There are variables that show the number of thresholds tested (N : 1,2,3, ...).The table below shows the optimal threshold value of each value of β that is used.

Table 5. Scenario 3 Test Result

β	FAR	FRR	Threshold
25	0.01	0.01	38.2680
50	0.01	0.01	38.2680
75	0.01	0.01	38.2680
100	0.01	0.01	38.2680

One threshold value selected is 38.2680 because it produces the lowest FRR and FAR. The bottom most FAR value specifies the lowest error rate to accept while the lowest value of FRR denotes the lowest refutation error. The optimal threshold value is determined by finding the intersection point between FAR and FRR. Scenario 4 testing result shows system performance using threshold value 38.2680 from the total of 150 test data belonging to 50 individuals with each amounted to 3 samples in the case of identification shown error rate of 1% and recognition rate of 99%.

D. Scenario 4

Based on the scenario 4, we conduct a test by observing the size variation of the palm vein image data. The initial size of the palm vein image data on the system was 256 x 256. This test is done by changing the data size of the palm vein image in order to observe the effect to the system accuracy. It is expected that better performance in terms of accuracy level can be achieved by adjusting the size of the image. The test was done using data model ratio and the ratio of 3:3 test data, threshold value of 0.53530564, and configuration of optimal parameters in scenario 1 and 2. Table 5 shows the test results for image data size variations.

Table 5. Scenario 4 Test Result

No	Image Size	Rate
1	152x152	84%
2	200x200	97%
3	256x256	99%
4	300x300	99%
5	320x320	99%

It can be seen that when we decrease the size of the palm vein image, the accuracy also decreases by around 13% and 2% for image sizes of 200 x 200 and 152 x 152, respectively. On the other hand, when we increase the size of the image, no changes in the accuracy is observed. In particular, the system has the same accuracy rate of 99 for image sizes of 256 x 256, 300 x 300, and 320 x 320.

VII. CONCLUSION

In this paper, we have optimized the DVHLBP method used for palm vein feature extraction [10], which can be more reliable and achieve higher accuracy as compared to previously proposed palm vein authentication systems [11]. Our proposed system has worked more leads to more accurate performance. We have also evaluated the performance of the optimized DVHLBP method in terms of the accuracy, FAR, and FRR. The accuracy has improved significantly compared with our previous method.

REFERENCES

- [1] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No 1.
- [2] Zhou, Y., & Kumar, A. (2010). Contactless Palm Vein Identification using Multiple Representations. Biometrika: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on Biometrika Compendium, IEEE
- [3] Mirmohamadsadeghi, L., & Drygajlo, A. (2011). Palm Vein Recognition with Local Binary Patterns and Local Derivative Patterns. Biometrika (IJC) International Joint Conference on Biometrika Compendium, IEEE
- [4] Mona, A. A., Hala M. E., El-Sayed M. E., & Abdel-Badeeh, M. S. (2013). Analysis of Palm Vein Pattern Recognition Algorithms and Systems. International Journal of Bio-Medical Informatics and e-Health, Volume 1, No.1.
- [5] Gopal, Smriti Srivastava, Saurabh Bhardwaj, Sandeep BhargavaaNetaji, Fusion of palm-phalanges print with palmprint and dorsal hand vein, Applied Soft Computing 47 (2016) 12–20.
- [6] Sachdeva, K., & Vinochia, O. P. (2014). A Comparative Study of Factors Affecting Performance of Local Binary Pattern (LBP) Variant along with Distance Metrics for Face Recognition. International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014.
- [7] Malik, D., Girgudar, D., Dahiya, R., & Sainarayanan, G. (2014). Reference Threshold Calculation for Biometric Authentication. IJ. Image, Graphics and Signal Processing, 2014, 2, 46-5.
- [8] Fischer, M., Rybnicek, M., & Tjoa, S. (2012). A novel Palm Vein Recognition Approach Based On Enhanced Local Gabor Binary Patterns Histogram Sequence. Systems, Signals and Image Processing (IWSSIP), 2012 19th International Conference.
- [9] G. K. M. Ong, T. Connie and A. B. J. Teoh, "A Contactless Biometric System Using Palm Print and Palm Vein Features," *Advances Biometric Technologies*, pp. 166-178, 2011
- [10] D.Fronitasari and D. Gunawan, "Palm Vein recognition by Using of Modified Local Binary Pattern for Extraction Feature, 2017 in 15th International Conference on Quality in Research (QIR) 2017, 2017.

- [11] Pooja1,Vinay Bhatia2 and Tanuja Dogra, "Palm Vein Recognition: An Advanced Biometric Technique for Authentication ",International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2016.

A Novel Framework to Improve Secure Digital Library at Cloud Environment

Heba Sayed

Hesham N. Elmahdy Fathy Amer
Faculty of Computers and Information,
Cairo University

Sherif Shaheen
Faculty of Arts

hobasyd@gmail.com

ehesham@fci-cu.edu.eg

dr_fathi_amer@yahoo.com

s_shaheen@cu.edu.eg

Abstract - Cloud computing is an advanced computing technology used by different organization or individuals for transferring, overseeing and storing over the internet. Security is an important issue that needs to be studied deeply and accurately when designing the digital library. Security shortcomings in libraries, combined with assaults or different sorts of disappointments, can prompt private data being improperly gotten to, or loss of honesty and integrity of the information put away. This paper will be introduced the concept and characteristics of cloud computing, the relationship between cloud computing and digital library will be analysis, the cloud computing security management problems under the environment of digital libraries will be studied , the availability level will be taken into research consideration while studying security management problems in digital library cloud computing. The main goal will be trying to present a possible solution for the preventing security threats and hackers on a digital library management system based on cloud computing.

Keywords-Cloud computing, Security, Digital library, Confidentiality, Availability, Integrity, Security threats.

I. INTRODUCTION

Cloud computing is a sophisticated technology designed to transfer processing and storage space that belongs to the computer to giant servers and then accessed through the Internet, Cloud computing has risen and emerged as a wonderful choice and better than traditional computing. It enables users to gain access to huge computing resources in an economical and efficient fashion. There are several cloud computing services and storage that offered by general storage provider companies, such as google apps services and amazon web services. A digital library can be defined as a technology for storing the knowledge and preserving data from loss to get it when needed, this data or knowledge can be found on different such as books, thesis, research documents, articles, audio and video. A digital library can give access to huge numbers of the information that is organized in the network over the world, which is an essential segment of any research experience.

By utilizing cloud technologies, library administrations can be made online without stressing over right versions of stages or the underlying technology. The proposed system aims to give multilevel security to the information over cloud, trying to provide an algorithm work against various attacks. So, we try to give a possible solution for the preventing security threats and hackers on digital library at cloud computing. The proposed Model used to design the digital library is the DELOS Reference Model. This model has 6 main components: the user, the content, the functionality, the architecture, the quality, and the policy [1]. The utility of this model is to offer a way to define digital libraries for DL designers.

A. Problem Statements

The digital library in the cloud computing environment faces the problem of data storage security, user information privacy and personal rights management, cloud data resource rights, The increasing volume of intellectual production and the diversity of its subject, and sources caused many problems which face researchers and information institutions, the most highlight of these problems are those related to give storage space for information, and variety of style treatments. In addition, problems related to information flow and the methods to be transmitted over the network without any loss of data, so security is an essential issue in digital library design. There are three factors that should be considered in the proposed work when constructing the security model for the digital library, they are confidentiality, integrity and availability.

Vulnerability in the safety system causes a weakness on the security system; these vulnerabilities are exploited to penetrate the security system by a threatened person who can perform unauthorized actions within the building cloud security system, by entering it in an unauthorized account or manner.

This research aims to develop techniques for building secure and scalable digital library systems based on cloud technology to serve large number of users by enhancing the cloud based services, library services and resources.

B. Motivation

The growing need for digital libraries to manage large amounts of data, these data need to be secured, so the security weaknesses must be studied carefully. As indicated by an investigation by the Oracle Corporation [2], information volumes are developing at 40% every year and by 2020 it will have developed to multiple times of its size in 2009. On the other hand, cloud computing promises the possibility for unlimited scalability. Also, the benefit of the cloud is that because of its ability to provision services on-demand, this is very important reasons. Security is an essential issue in digital library design because of various attacks.

Security vulnerabilities in digital libraries [3], suffering from types of attacks that can lead the failure on the library system; it can lead inappropriately access to confidential information. These [3] thus can amazingly affect the trust of the publishers or other content providers.

II. LITERATURE SURVEY

Cloud computing security challenges have been widely researched, Lingling Han [4] gave a new advanced library stage used to tackle the issue of library resources putting away and sharing to give quick, protected, helpful and proficient administrations to clients. Goyal [5] characterized the advantages and examinations of cloud computing administrations on the parameters of valuing, most extreme point of confining, information security, and information reinforcement. Qingjie MENG [6] defined cloud computing method of library computerized assets, cloud key appropriation plan to adjust to library applications was displayed, the improved customary PKI, the PKI-based distributed computing correspondence and security assurance components for the library are presented. Library distributed computing key dissemination, confirmation and encryption strategies, increasingly secure homomorphic encryption component for library data recovery. Surendra [7] talk about the Cloud Computing in libraries, how make viable library benefits of distributed computing, Issues, Challenges and Benefits of distributed computing. Varun [8] delineated a concise portrayal of what precisely cloud computing security-related issues are, and talks about information security and security assurance issues related to cloud computing over all phases of information life cycle. Demonstrating, the current answers for information security and protection assurance issues in the cloud. What's more, depicts future research work. Guo Xin [9] dissected the idea of cloud computing and related innovation, presented the necessities of the development of computerized library, talked about how to plan the engineering of Digital Library Based on distributed computing. Dev Ras [10] described the architecture of cloud computing to building and managing libraries, tried to make progress current user service model in the university library by using Cloud Computing. Tamanna [11] proposed a procedure for information classification in cloud condition, concentrated on describing the information considering the security essentials of the data that separates the information into basic, confidential and highly confidential utilizing improved machine learning calculation.

Nabeil Eltayieb et al [12] presented an attribute based secure information sharing (ASDS) conspire for cloud condition, which gives information access control, confidentiality, information validation, and adaptable client denial. Also, the proposed plan can oppose intrigue attack and replay assault. The examination of security properties and the correlation execution with other information sharing plans have exhibited that ASDS is truly reasonable for cloud condition.

III. TECHNOLOGY DESCRIPTION

The goal of this section is to go through the definition and benefits of cloud computing, then illustrated the security problems of digital library under the environment of cloud computing , finally studying different security threats that affect cloud computing.

A. Cloud Computing Definition

There are many definitions of cloud computing, one of these definitions refer to NIST that define the cloud computing as " Distributed computing is a model for empowering helpful, on-request arrange access to a common pool of configurable figuring assets (e.g., systems, servers, stockpiling, applications, and administrations) that can be quickly provisioned and discharged with insignificant administration exertion or specialist organization cooperation, this definition is the most broadly used [8].

B. Benefits of Cloud Technology

The benefits of Cloud Computing are that it offers colossal measures of power regarding figuring and capacity while offering improved scalability and flexibility. In addition, with effectiveness and financial matters of scale, Cloud technology administrations are getting to be a less expensive arrangement [13].

On-demand self- service, Autonomous System, Scalability and flexibility, and , shared resources are some of the essential characteristics of cloud computing that separates it from each other technologies[13][14].

C. Cloud Computing Security Management Problems for Digital Library

The motivation behind the digital Library Management framework is to take into account putting away subtleties of an expansive number of books, magazines, Journals and theory. Therefore, there are some great issues that need to be referenced when allowing moving sensitive data and application to the public cloud environment. Most of organizations prefer to use cloud computing, but it still suffers from some weaknesses.

D. Threats of Cloud Computing

There are some security threats that have an effect on a cloud computing, this research will be mention some of these threats and then covered some of them:

- Data Loss: Data loss can have large effects monetarily, operationally and even lawfully as data loss may result in the inability to meet consistence strategies or information security prerequisites.
- Data Ownership & Control: Moving to the cloud implies that the service provider or organization could have some level of access to your information.

- Data Breaches: Data breach threats exist whether data is stored internally or on the cloud, some cloud administrations might be increasingly vulnerable against potential attacks and the hijacking of information because of new strategies for assault.
- Malicious Attacks & Abuse: hackers or even approved clients may conceivably assault and abuse cloud storage for illicit exercises. Examples of malicious threats include:-
 - a. standard specifications
 - b. Insider breaches and hacks
 - c. Theft of proprietary data or intellectual property
 - d. Industrial espionage or IT sabotage
 - e. Fraud
 - f. Improper disposal of documents or leaving doors unlocked.
- Insider Threat: Insider threat comes from people within the organization; This can lead to the misuse of important data. Insiders are frequently familiar with the association's information and intellectual property as well as the techniques that are set up to ensure them.
- Unauthorized Access: Unauthorized access could be happened when someone tries to reach to a website or an area of a system by using someone else's account or other methods. For example, if somebody kept easy to guess password. Some framework managers set up alarms to tell them when there is an unauthorized get to endeavor, with the goal that they may explore the reason. These cautions can help prevent hackers from accessing a safe or private framework. Many secure frameworks may likewise bolt a record that has had too many fizzled login endeavors.
- Distributed Denial of Service Attacks (DDOS): is attacked by dumping sites with a torrent of unnecessary data is sent via infected devices and with the wide spread of the Internet Denial of service has become more exciting for hackers.

IV. MODEL AND DESIGN FOR DIGITAL LIBRARY

The new security design of the digital library system must contain at least one addition to previously designing systems. Proposed design model that will be introduced on digital library is a DELOS Reference Model that has 6 main components in a digital library: content, user, functionality, architecture, quality, and policy. We introduce the security issue of the two layers of this model: the user and the content security issue. The utility of this model is to provide a way to define digital libraries for DL designers. In this section, the following question will be studied: What are the security issues that need to be measured to secure the digital library?

A. Proposed Model

The proposed system aims to give multilevel security to the information which is flowing over the cloud, also provides a degree resistance against various attacks. So, this research will present a possible solution for preventing security threats and possible vulnerabilities on a digital library system at cloud computing platform

- The covered threats are:

1. Unauthorized access
2. Session hijacking attack
3. Denial of service attack (DDOS)
4. Cross-site Scripting (XSS)
5. Blocking Brute Force Attacks
6. SQL Injection

7. Device Cookies.

All Covered Threats are dealing with public cloud on platform as a service model.

- The security Level will be covered:

1. Three layer to log in
2. Hide admin login page
3. Password Authentication Delay
4. Using CAPTCHAS
5. Verification code
6. Alternate XSS Syntax
7. XSS using code encoding
8. XSS using Script via Encoded URI Schemes

Figure 1 describe the details of the proposed model, in this figure apply the security threats on digital library in the three cases : Admin account, user account, database account under the Public cloud environment on platform as a service model

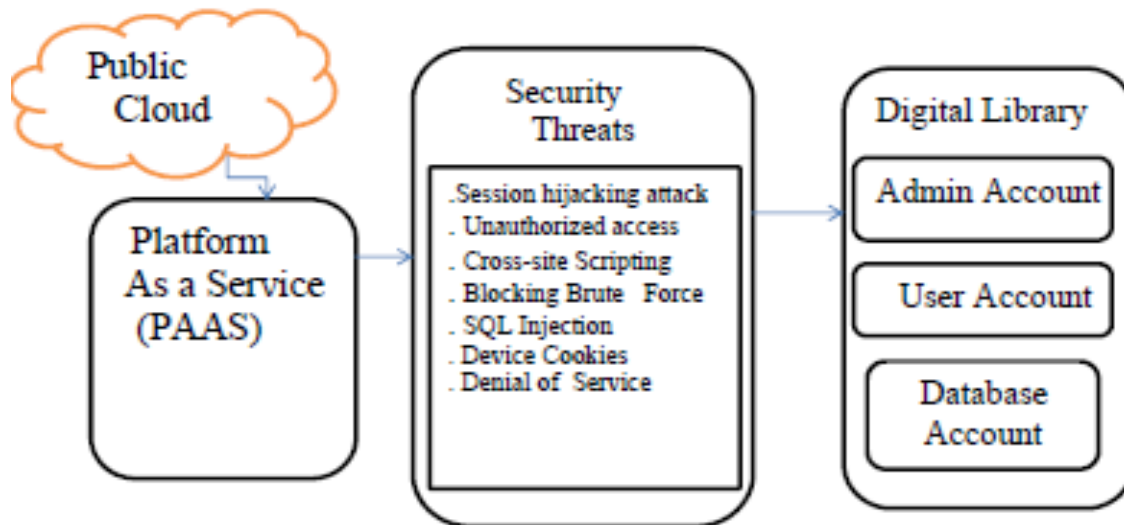


Figure1 :

Proposed Model

Knowing that , the cloud library management system was implemented according to the standard specifications in PHP, html, Apahe server and Mysql by using Xampp server.

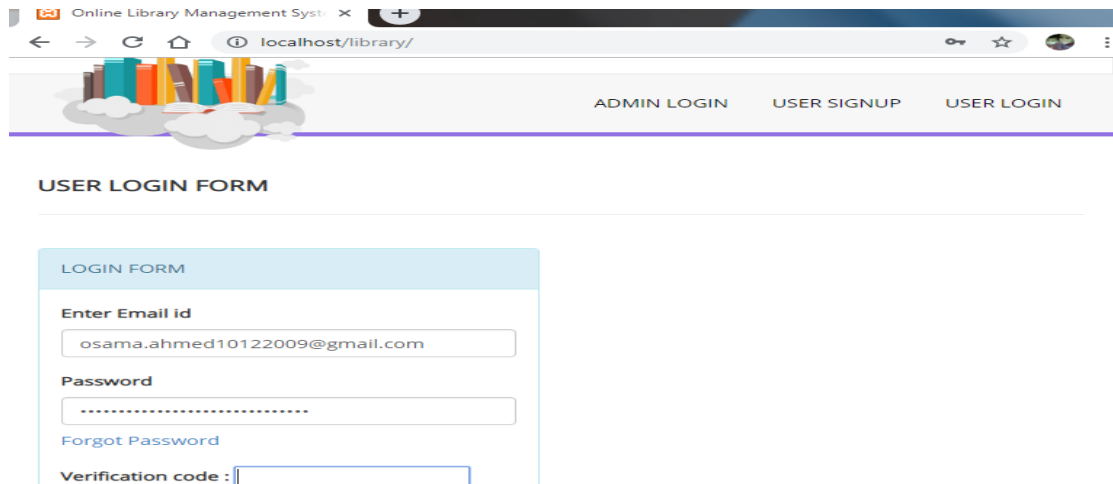
V. EXPERIMENTS AND RESULTS

According to DELOS Reference model, there are two security requirements for accessing the contents of the digital library:

Firstly : - the authentication: the end user must register to the system first to have an ability to log on to the library framework.

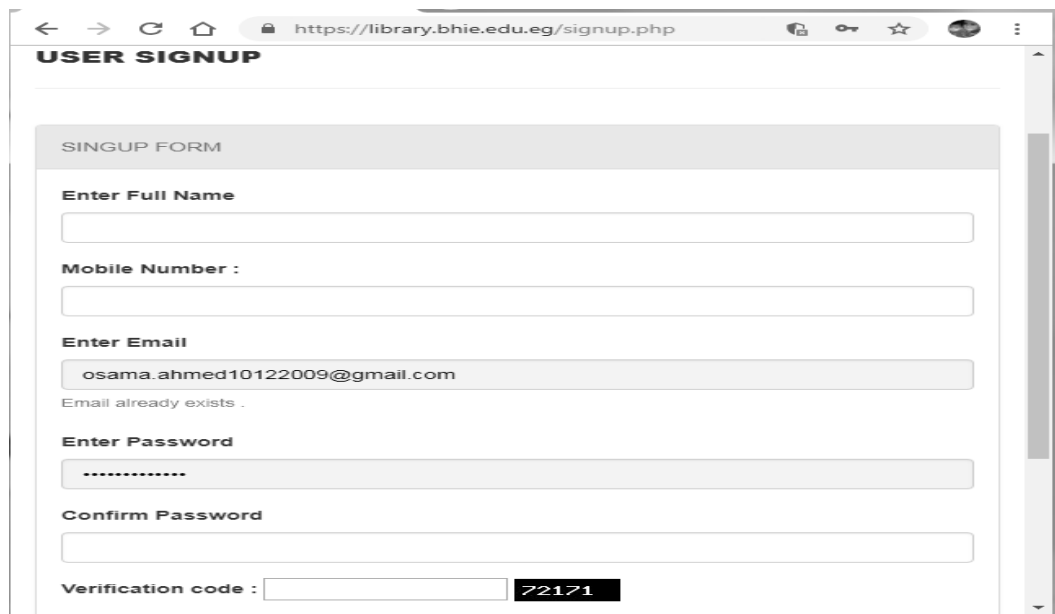
Secondly: - the confidentiality: Preventing unauthorized access to the data by encrypting the content using encryption algorithm.

The proposed frameworks for online digital library system under the environment of cloud computing are shown in figure 2 , 3 and 4. The figure 2 shows the home page for cloud library system, on this page we can go to the rest of the pages after registration and after achieving security metrics "confidentiality, integrity, availability", After using Bluehost account to reserve space on the cloud.



The screenshot shows a web browser window with the address bar displaying 'localhost/library/'. The page title is 'Online Library Management System'. The navigation bar includes links for 'ADMIN LOGIN', 'USER SIGNUP', and 'USER LOGIN'. The main content area is titled 'USER LOGIN FORM' and contains a 'LOGIN FORM' box. Inside this box, there are input fields for 'Enter Email id' (containing 'osama.ahmed10122009@gmail.com'), 'Password' (masked with dots), and 'Verification code :'. There is also a 'Forgot Password' link.

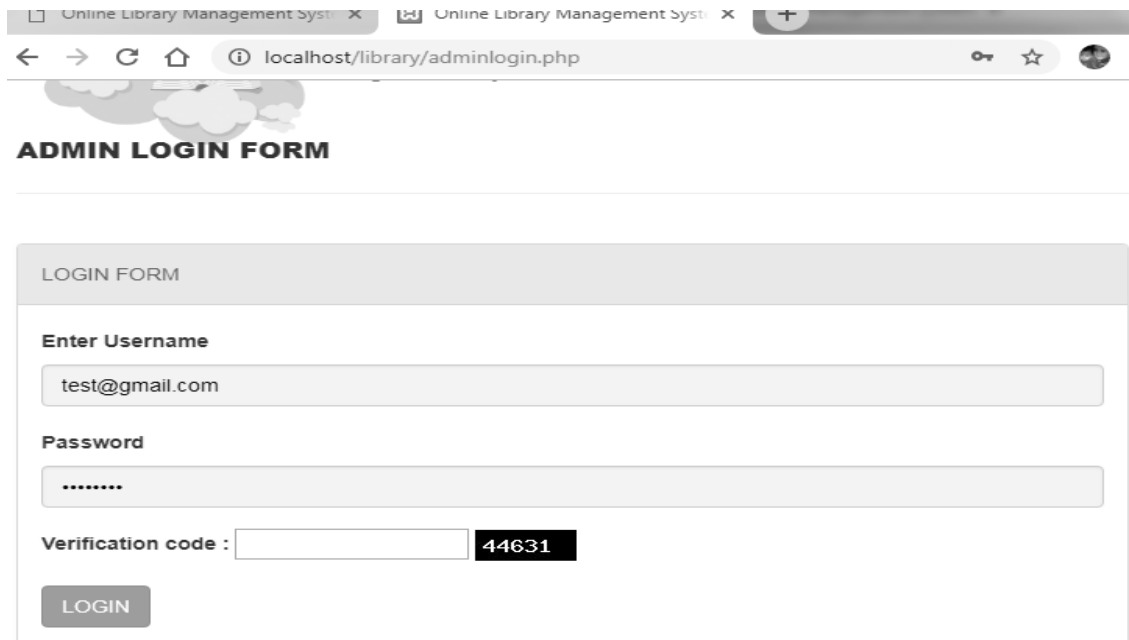
Figure 2: Framework for Cloud Library Management System



The screenshot shows a web browser window with the address bar displaying 'https://library.bhie.edu.eg/signup.php'. The page title is 'USER SIGNUP'. The main content area is titled 'SINGUP FORM' and contains input fields for 'Enter Full Name', 'Mobile Number :', 'Enter Email' (containing 'osama.ahmed10122009@gmail.com' with a message 'Email already exists .'), 'Enter Password' (masked with dots), 'Confirm Password', and 'Verification code :'. The verification code '72171' is displayed in a black box.

Figure3: Registration Page for Cloud Library System after Applying Security Threats

In the figure3, if the end user tries to go to admin page, he will get this message "Invalid Details", This is one of achieving the security requirements to prevent attackers Penetrates the library system. The admin has the authority to add, update and delete categories, books and authors.



Online Library Management System x Online Library Management System x

localhost/library/adminlogin.php

ADMIN LOGIN FORM

LOGIN FORM

Enter Username

test@gmail.com

Password

.....

Verification code : 44631

LOGIN

Figure 4: Admin Login Page (end user or hackers cannot go to admin page)

This approach is differed from other approaches because it is a new idea to measure and evaluate a security of online digital library system using quantitatively metrics to decide the advantages of proposed algorithm. Each of this security metrics has threats that are affected on it. To achieve the integrity metric, we can prevent unauthorized access to make change, deletion or addition of the data saving on cloud library by using three layered to login. The results of the experiment are shown in figure5 and figure6.

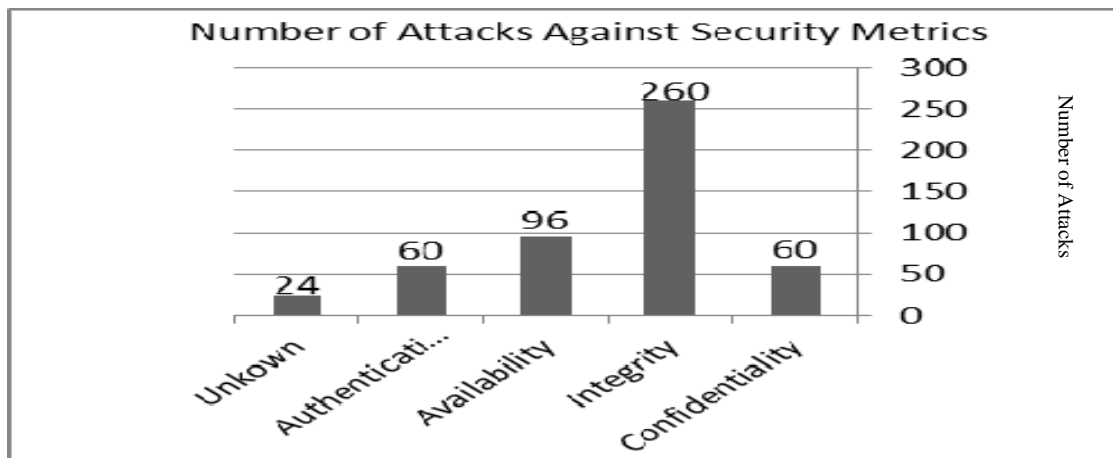


Figure 5: Security Evaluation

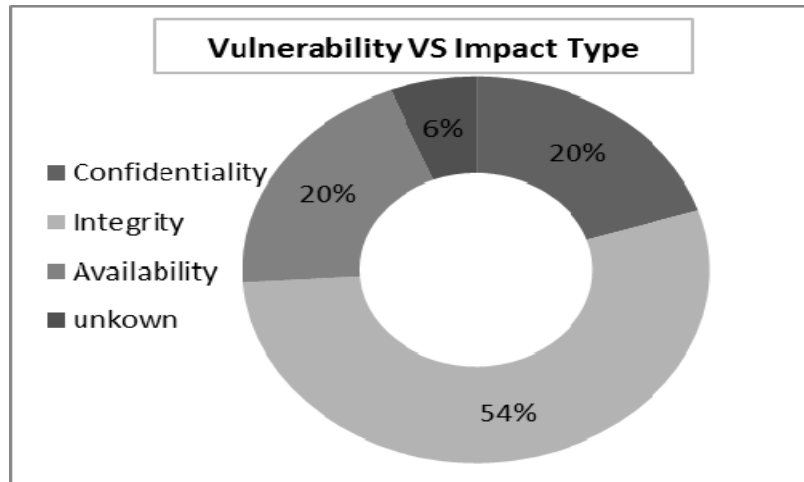


Figure6: Vulnerability VS Impact Type

In these two last figures, threats to integrity are the highest one, so the integrity is on the risk. According to the above results, to apply more security for cloud data storage and solving the problem of integrity, making these steps:-

- Always encrypting sensitive data.
- Taking the necessary preventative measures to ensure your systems, networks and applications are secure.
- Taking a backup of the data, continuously.
- Using multiple layers to log into the system of cloud library to prevent unauthorized access
- Using protection technology on the integrity such as watermarks, digital signatures, finger prints
- To achieve authentication and integrity, using remote desktop to grantee that the admin did not work from home.

VI. COMPARISON ANALYSIS

In this section, various approaches for constructing secure digital library illustrated on table1. The comparison analysis between the existing approaches and our scheme in terms of security metrics are illustrated on table2.

TABLE I

Comparison between different digital library models

Digital library model	Objective	Techniques used	Benefits	Cloud model
Ipoulo_2013, Cloud Computing for Digital Libraries[15]	Achieved secured data on public cloud	AWS using java to develop typical digital library services	Save time, money, High scalability	IaaS, Public cloud
Martine Bellaïche, Security in cloud computing [16]	Deploying a secure application on AWS	AWS Using simulation such Cloudsim	enhance the energy saving capabilities	IaaS,
Elsherbiny2011	scalable and flexible	SSL Model to generate DL	Generation of DL using SSL	Did not consider , but PaaS can be used
Online DL Mangement system, (new proposed)	Multi- level To achieve confidentiality, integrity, availability	Online Digital library framework using DELOS Model using Bluehost account	Easy to test application, cost effective	PaaS, Public cloud

TABLE II

Comparison between proposed scheme and other existing scheme in terms of security metrics

scheme	Security Achievement	Confidentiality	Integrity	Availability	Approach used
--------	----------------------	-----------------	-----------	--------------	---------------

Elsherbiny2011, "Secure Digital Library"	Medium, using 5S scheme	Achieved using different security mechanism on each SSL	Considered on streams, structures, societies.	Considered on Scenarios model using different security mechanism such as firewall	SSL Model, there are security attacks for each model.
Kulwinder Kaur et al. 2016 [17]	Medium, using classification of data to secure sensitive data	Classifying the data into confidential & non confidential	Using hashing approach to achieve integrity	Mentioned but not considered	Data classification using machine learning algorithm
Anupama 2017 [18]	High	Replicated the data among different cloud	Using Hash based message authentication	Data stores on multiple cloud	Data replication
Eltayieb et al.2019 [12]	Achieve: access control, data confidentiality, authentication, integrity, and flexible revocation	manager encrypts data before sending to the cloud	Mentioned but not studied	Mentioned but not studied	New scheme attribute-based secure data sharing (ASDS)
Our scheme	Highly, more security Achieved: confidentiality, integrity, High availability level	Using hybrid security algorithm to prevent unauthorized person to access data	Using hashing function, different protection technology to prevent modification	Achieved on "architecture" using replication to solve the problem of DOS attack	DELOS Reference Model, Multiple layers of security plus encrypted sensitive data to prevent security threats

VII. CONCLUSIONS

The motivation behind the library management framework is to take into consideration putting away subtleties of an expansive number of books, magazines, Journals, postulation and take into account include, seek, get, return offices independently to head/Librarian, staff and students.

This research has been studied cloud computing security management problems and apply it on online digital library framework to make it secure. Cloud computing is the innovation of present and future, To carry out new encryption and decryption technique for overcoming the hackers and intruders knowledge to give protect to the cloud storage data on digital library, we proposed the DELOS Reference Model for digital library, this model has 6 main definitions, each of these definition needs some security requirements. There are three factors that should be considered in the proposed work when constructing the security model for the digital library, they are confidentiality, integrity and availability.

The proposed system aims to give multilevel security to the information over cloud, and trying to provide an algorithm works against various attacks. So, we presented a possible solution for the preventing security threats and hackers on digital library at cloud computing.

In the future, it is possible to expand digital library work on the cloud by more studying of scalability of stored data, and it may be able to store a larger amounts of data. On the other hand, it is possible to Served large number of users by enhancing the cloud based services, library services and resources by using any simulation techniques such as Cloudsim simulator.

REFERENCES

- [1] Candela, L., et al. *The DELOS Digital Library Reference Model*. 2007
http://www.delos.info/index.php?option=com_content&task=view&id=345
- [2] Dijcks, J.-P. Oracle: Big Data for the Enterprise. Oracle White Paper, 2012.
- [3] Edward Fox and Noha ElSherbiny (2011). Security and Digital Libraries, Digital Libraries - Methods and Applications, Dr. Kuo Hung Huang (Ed.), ISBN: 978-953-307-203-6, InTech, Available from: <http://www.intechopen.com/books/digital-libraries-methods-and-applications/security-and-digital-libraries>
- [4] Lingling Han and Lijie Wang, "Research on Digital Library Platform Based on Cloud Computing ", pp. 176–180, 2011.
- [5] Goyal, S. (2012). A comparative study of cloud computing service providers. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(2), 1-5.
- [6] Qingjie MENG, Changqing GONG , "Research of cloud computing security in digital library" ,6th International Conference on Information Management, pp:41- 44 , 2013.

- [7] Surendra Kumar Pal, "Cloud Computing and Library Services: Challenge & Issues" , September 2014.
- [8] Varun Krishna Veeramachaneni, "Security Issues and countermeasures on Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 4, Issue 5, pp:82-93, September 2015.
- [9] Guo Xin, "Analysis of Key Technologies of Digital Library Based on Cloud Computing" , International Conference on Education , pp 695 - 698, 2016.
- [10] Dev Ras Pandey, Gauri Shanker Kushwaha, "Cloud Computing for Digital Libraries in Universities", International Journal of Computer Science and Information Technologies, Vol. 6 (4) ,pp: 3885-3889, 2015.
- [11] Tamanna, Rajeev Kumar, " Secure Cloud Model using Classification and Cryptography" , International Journal of Computer Applications, Volume 159 – No 6, February 2017.
- [12] Eltayieb N, Wang P, Hassan A, Elhabob R, Li F. ASDS: Attribute-based secure data sharing scheme for reliable cloud environment. *Security and Privacy* 2019;2:e57. <https://doi.org/10.1002/spy2.57>
- [13] Shawish, A. and Salama, M. (2014) Cloud Computing: Paradigms. Inter-Cooperative Collective Intelligence: Techniques and Applications, Studies in Computational Intelligence 495, Springer-Verlag, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-35016-0_2
- [14] L. Wang, and G. Laszewski, "Scientific Cloud Computing: Early Definition and Experience," in Proc. 2008 10th IEEE International Conference on High Performance Computing and Communications, Dalian, China, 2008, pp. 825 – 830
- [15] L.Poulo, "Cloud Computing for Digital Libraries", Department of Computer Science University of Cape Town, 2013.
- [16] Martine Bellaïche, "Security in cloud computing", Polytechnic University of Catalonia, 2016.
- [17] Kulwinder Kaur, Vikas Zandu , "A Secure Data Classification Model for achieving Data Confidentiality and Integrity in Cloud Environment", International Journal on Computer Science and Engineering, Vol. 8 No.9, Sep 2016.
- [18] Anupama Prasanth, " Cloud Computing: Secure and Scalable Data Access Security Models", International Journal of Computer Applications, Volume 170 – No.4, July 2017

(IJCSIS) International Journal of Computer Science and Information Security,
Vol. 17, No. 5, May 2019

Botnet Detection and Prevention in Software Defined Networks (SDN) using DNS Protocol

Paper

By

**Muhammad Junaid Zafar, Riphah International
University, Islamabad, Pakistan**

mjunaidzafar@hotmail.com,

**Professor Dr. Muhammad Zubair, Riphah International
University, Islamabad, Pakistan**

m.zubair@riphah.edu.pk

Abstract

Software defined networks (SDNs) is one of the most emerging field and will cause revolution in the Information Technology (IT) industry. The flexibility in the SDNs make it most attractive technology to adopt in all type of networks. This flexibility in the network made the SDNs more prone to the security issues so it is important to cater these issues in start from the SDN design up-to the deployment and operations. This Paper proposed a DNS based approach to prevent SDNs from botnet by applying one million web database concept without reading packet payload. To do any activity, Bot need to communicate with CnC and requires DNS to IP resolution. For any request having destination port 53 (DNS) will be checked. The protocol will get all matching traffic and will send it to 1Mdb. If URL Exists in 1Mdb then do not respond otherwise send reply with remove flow and block flow to the controller. This approach will use Machine learning algorithms to classify the traffic as BOT or normal traffic. Naive Bayes Classifier is used to classify the data using python programming language. The selection of dataset is very important task for machine learning based botnet detection and prevention techniques. The poor selection of dataset possibly lead to biased results. The real world and publically available dataset is a good choice for evaluation of botnet detection techniques. To meet these criteria, publicly available CTU-43 botnet dataset has been used. This dataset provide packet dumps (pcap files) of seven real botnets (Neris, Rbot, Virut, Murlo, Menti, Sogou, and NSIS). We will use these files to generate botnet traffic for evaluation and test our model. To generate normal traffic, we selected ISOT dataset. This dataset provides a single pcap file having normal traffic and traffic for weladec and zeus botnet.

Contents

1	Introduction	7
1.1	Problem Area	8
1.2	Problem Statement	8
1.3	Research Questions	8
1.4	Research Objectives	8
1.5	Significance of Work and Potential Benefits	9
1.6	Novel Contributions	9
1.7	Chapter Summary	9
2	Literature Review	10
2.1	State of the Art	10
2.2	Limitation of Existing Techniques	21
2.3	Chapter Summary	22
3	Proposed Solution	23
3.1	Proposed Solution Architecture Components	23
3.1.1	End User	24
3.1.2	SDN Controller	24
3.1.3	Flow Collector	24
3.1.4	Feature Extractor	25
3.1.5	Classification Module	25

3.1.6	One Million Good Websites database	25
3.1.7	Log Analyzer	25
3.1.8	Dataset	25
3.2	Comparison	30
4	Methodology, Implementation and Results	31
4.1	Deployment and Implementation	31
4.1.1	Flow Chart	31
4.1.2	Implementation	33
4.1.3	Algorithm	33
4.2	Results	34
4.2.1	Traffic List	34
4.2.2	Top One Million Web Site Database	35
4.2.3	Selected Protocol List	36
4.2.4	DNS Query	37
4.2.5	Results	38
4.3	Future Work	40
	References	41

List of Figures

3.1	Proposed Solution Architecture Components	24
3.2	CTU-43 Dataset	27
3.3	ISOT Dataset	28
3.4	One Million DB Dataset	29
3.5	Comparison	30
4.1	Flow Chart	32
4.2	Actual User Traffic	34
4.3	Top One Million Database	35
4.4	Selected Protocol List	36
4.5	A DNS Query	37

List of Tables

List of Abbreviations and Symbols

Abbreviations

CNC	Command and Control
SDN	Software Defined Networks
DNS	Domain Name System
1Mdb	One Million Database

CHAPTER 1

Introduction

Software-defined networking (SDN) is an architecture that aims to make networks agile and flexible. The goal of SDN is to improve network control by enabling enterprises and service providers to respond quickly to changing business requirements. In a software-defined network, a network engineer or administrator can shape traffic from a centralized control console without having to touch individual switches in the network. The centralized SDN controller directs the switches to deliver network services wherever they're needed, regardless of the specific connections between a server and devices. A typical representation of SDN architecture comprises three layers: the application layer, the control layer and the infrastructure layer. The application layer, not surprisingly, contains the typical network applications or functions organizations use, which can include intrusion detection systems, load balancing or firewalls. Where a traditional network would use a specialized appliance, such as a firewall or load balancer, a software-defined network replaces the appliance with an application that uses the controller to manage data plane behavior. The control layer represents the centralized SDN controller software that acts as the brain of the software-defined network. This controller resides on a server and manages policies and the flow of traffic throughout the network.

This document covers and introduced a technique to secure the SDN from BOTs using a new method. The document covers the detail of software defined networks, BOTs, existing techniques used to detect and protect SDNs from BOTs, issues in existing techniques used to secure SDNs from BOTs and new technique introduced to secure SDNs from BOTs.

1.1 Problem Area

Security is one of the main concern in Software Defined networks due to the centralized controlled nature of the solution. It is very important to secure the controller from all type of threats. One of the major threat for SDN is to protect the SDN and SDN Controllers from BOTs. If not secured and in case controller compromised then whole network will be compromised considering that controller is controlling the whole network.

1.2 Problem Statement

Security of SDN from BOTs and BOTNETs is very important. It is very important to detect the BOTs in very start of communication before the BOTs damage the network. In case BOTs successful in communication with the Command and Control Center (CnC) then it will get the execution command from the CnC and will cause security issues in the SDN and can take over the controller control as well to get the complete control of the network. It is very important to secure the SDNs from BOTs.

1.3 Research Questions

1. What are the limitations in existing BOTNET detection and prevention techniques.
2. What are the ways to stop the BOTs in start of communication before it damages the Software Defined Networks.
3. What are the ways to stop the BOT to contact with their CnCs.
4. Which protocol is the best to detect BOTNET communication.

1.4 Research Objectives

Software Defined Networks (SDNs) are effected by BOTs and damage the network once compromised by BOTs. Existing techniques can detect the BOTs in SDNs but have some limitations due to which limited or high impact damage to the network can occur. Objective of the research done in this Paper is to introduce a new technique for detection and prevention of BOTs in Software defined network using DNS protocol. The new technique have some benifits to overcome the limitations of existing techniques. This

will secure the SDNs completely from BOTs in very start of communication.

1.5 Significance of Work and Potential Benefits

The approach have a lot of benefits as compare to other approaches i.e. Very less computations on live traffic, Only Traffic for Port 53 will be monitored, No computation or processing on remaining traffic, Bots will be blocked at very start of communication, Infected IPs will be permanently blocked, System not only provide detection but also prevention solution, standard Technique for all type of controllers and protocols, isolate infected system before start of communication.

1.6 Novel Contributions

A detailed literature survey has been performed with near about 40 papers have been studied, 10 very focused on the topic and research questions are selected. Limitations of existing research has been addresses in the proposed methodology which will have a great contribution in the research area. The proposed methodology is completely different and new which has been never proposed or opted before in any of the research paper found during literature survey.

1.7 Chapter Summary

It is very important to cater the issues of BOTs in Software defined networks. The Paper identified issues and limitations found during literature survey and review in existing techniques. A problem statement has been identified and a new technique has been proposed to cater the limitations of existing techniques. The new technique and methodology proposed in this Paper will have a great positive impact in the research area for this specific identified problem area.

CHAPTER 2

Literature Review

A detailed literature survey has been performed having literature review of approx. 40 papers and approx. 10 of these are selected which are most recent, having impact factors and which are most related to the problem statement. Existing research has been systematically analyzed in breadth and depth. These papers are selected by the process of literature comprehension. Detail of selected papers is given below:-

2.1 State of the Art

A detailed working on the security of SDN Controllers has been done in [1] with a detailed introduction of Software Defined Networks, definition of controllers, Application programmable interfaces and recommendations to improve SDN Controller security. The concept of thesis is based on splitting the network intelligence out of the packet switching device and putting it into a logically centralized controller. The forwarding decisions are made by the controllers, which are located into the switches via standard protocols, like Open-flow. Thesis also discussed a comprehensive literature review concerning SDN controllers security has been done. Demonstrate a comprehensive studies on SDN by clarifying its concepts, Open-flow protocol architecture and how it works [1].

A discussion on SDN controllers and several threat Vectors which may enable for the exploitation of vulnerabilities of SDN Controllers. Designing a dependable Controller platform including the requirements for a secure, resilient, and robust SDN Controller. How we can secure SDN controllers by making recommendations for security improvements for future SDN Controller. Existing gap between the actual security level of the

current SDN Controller design and the potential security solutions. controllers securities are addressed by employing detection system to help in identifying any abnormal flows, trust model used with multiple trust anchor certification authorities and use of cryptography across controllers to secure the communication. Rule-chain Conflict Analysis (RCA) has been used for detecting the occurrence of any conflict [1].

Thesis concluded on the recommendations to improve the security of SDN Controllers with three design recommendations i.e. (1). based on software security principles (2) Secure default controller setting: Safe mode boot processes (3) Application Future Proofing [1].

Botnet classification using centralized collection of network flow counters in software defined networks has been proposed in [2] for the detection of botnets in software defined networks. The paper defined the bot-nets as a network of bot-malware infected machines controlled by bot-master is one of the top listed cyber security threat. Botnets are the most advance family of malwares and continuously changing to evade detection techniques. To cope up with changing nature of botnet, the detection techniques need continuous improvement and integration into new technologies. The latest techniques in botnet literature are targeting network header information only to classify botnet behavior using machine learning approaches. Paper also defined Centralized network flow collections as one of the major challenge in these techniques. The paper propose a botnet detection in SDN by collecting centralized network flow statistics in form of OpenFlow counters. The proposed approach apply C4.5 decision tree based supervised classification algorithm on collected counters. OpenFlow counters are suitable candidate to provide a good feature set to distinguished network behavior patterns of bot-malware. Paper also discussed the history of botnet, botnet impelled in early 90s from egg-drop application written to manage Internet relay chat (IRC) network. The botnet start with the same idea of centralized architecture and IRC protocol as used in eggdrop. These early botnets having centralized architecture disclose there c2c servers and are vulnerable to single point of failure. The centralized botnet introduce intermediate layers to hide c2c servers. The botnet change with time and introduce distributed and hybrid architecture. The work proposed in show evolving trend of botnets. The paper proposed detection model with Implement supervised decision tree based botnet detection technique into SDN Evaluate if OpenFlow counters provide enough statistics to detect botnet patterns. C4.5 supervised decision tree algorithm Used and train the model with

publically available botnet datasets. Approach consist of three stages .i.e (i) Centralized collection of OpenFlow counters from SDN controller (ii) Feature set extraction from collected counters (iii) Apply C4.5 supervised machine learning algorithm to classify flows into botnet flows or normal flows [2].

Work proposed in [3], apply three different supervised classification algorithms. The focus of the approach is to detect c2c servers therefore the technique first isolate server flows from incoming flows based on open listening ports. The server flows fed into all three detection algorithms for evaluation. The flow sized based, client access pattern based and temporal behavioral based features used in these detection algorithms. Another approach evaluate different flow intervals with proposed model and shows optimum results for flow monitoring interval. The work also include two botnet samples (Weladec and Blackenergy) in testing dataset to evaluate if their detection model is capable to cope up with unknown botnets. The evaluation results show that the model is capable to detect unknown botnets [3].

The work proposed by matija evaluate eight different supervised MLAs. The approach uses 39 different flow features for training and detection of bot malware patterns in provided dataset [3]. The proposed detection system in [4] evaluated with only two samples of Weladec and Storm botnets. The approach shows very promising results. The work proposed in revisit network flow features used in machine learning based botnet detection techniques. The approach uses a dataset comprising of 16 different botnet samples. The dataset generated by combining three different real world datasets including ISOT dataset, ISCX 2012 IDS dataset, and botnet dataset of malware capture facility project. The approach evaluate different set of network flow features with this dataset. The botnet literature only have few proposed techniques that explore SDNs. These techniques collect flows from individual networking elements as applied in classical network and none of these techniques explores OpenFlow counters for botnet detection. The work proposed in COFFEE explore SDN for botnet detection. The approach work in two phases. The first phase collects netflows from individual forwarding elements and analyze to detect potential botnet flows. This approach proposed to use the same flow feature set as used in [4]. The second phase collect payload for the detected flows by using SDNs dynamic programmability. This phase classifies detected flows into botnet or normal. The work proposed in explore SDNs for botnet detection. The proposed approach used IPFIX flow protocol to collect network flows from each forwarding ele-

ments. The approach does not share evaluation results [4].

Paper in [5] presents the review of SDN security and potential threat against botnet Attack. It defines the BOTNET Definition, SDN Definition, CIA Definition, BOTNET Prevention in SDN, At the end of this paper, a future research to handle botnet attack. Paper also define the potential attack on SDN which includes Unauthorized Access, Data Leakage Access:- There is some possibilities attacker disguised as controller or application from a 3rd party. An attacker could get access to network resources and control the network operation and Data Leakage Packet handling: - SDN has several potential actions such as forwarding, drop, and send a packet to the controller. With this system, there is possibility attacker to determine the action to the specified packet by determining time process for packet arrived because packet forwarding from packet handling to the controller is longer than others. Other attack discussed are Data. Modification: - Attacker modify data whenever they can hijack controller. Attacker modify an inject flow rules in network devices, Malicious Application:- Because of SDN open for 3rd party application to the architecture, some application could be exploited by an attacker and drive into the unsafe state, Denial of Services, Configuration Issues:- SDN as the programmable network has weakness in security because it can come to be vulnerable especially for data or control communication and System Level SDN Security Its important for an operator to know the mode and switch activated in connection disruption, forwarding pattern during failures, the effect on flow entries and pattern of the controller when reestablishing the connection. Paper provided SDN Defense Mechanism against Botnets that includes generally, methods that have been done before on traditional network are based on the habit and pattern of network traffic. Paper discusses 5 main components with the following explanation: (i) Traffic Flow and Feature Extractor Module At this stage, the network traffic from different hosts is classified with the aim of obtaining information obtained from network flow, (ii) P2P Application Detection Module This module has the main purpose of obtaining the vector feature. In the process this module is divided into 4 sections as follows: (a) Building Detection Model and Training set (b) Feature Selection (c) Classifier (d) Traffic Analysis. (iii) Report to OpenFlow Controller. If the classification result of the detection agent matches the class on the P2P botnet, the detection agent will inform the rule arbitrator to adjust the flow entries in the data link bridges. (iv) Flow Rule Modify on OpenFlow Switch Once the Rule Arbitrator receives a RESTful HTTP request sent from the detection agent,

the flow table will be modified by a RESTful HTTP request in the data-link bridges.
(v) Drop, Forward, or Redirect Packet [5].

Paper in [6] discussed the Machine learning based botnet detection in software defined networks. It used the flow based approach to detect botnet by applying machine learning algorithms to software defined networks without reading packet payload. Uses network flows as input and process it in two windows based modules to extract a statistical feature set to be used for classification. The first module process network flow stream to extract flow traces. The window size of this module is 10 which means a flow trace with 10 flows is considered as a trace of interest and forwarded to the next module for further processing. The second processes selected trace and fetches historical flows in last 60-minute window for the source and destination IPs of the trace. feature set is extracted from selected trace and relevant historical flows. The approach applies supervised decision tree based machine learning algorithm to create a model during a training phase using extracted feature set. This model is then used to classify flow traces during the testing phase. dataset for experimentation is extracted from publicly available real botnet and normal traces. The experimental findings show that the method is capable to detect unknown botnet. The results show detection rate of 97 percent for known botnets and 90 for unknown. The paper proposes to use intelligence from both real-time flow stream and historical context of a flow trace to extract a more meaningful feature set to help classification process. C4.5 a decision tree based supervised machine learning algorithm for botnet classification. The proposed approach operates in two modes the training mode and test. This is used to train the C4.5 algorithm to recognize botnet behavior patterns with help of labeled dataset. A decision tree model is created based on training during this mode. The testing uses pre-computed model to classify flow traces. The botnet are collected from publicly available CTU-13 dataset and ISOT. For normal traffic representation, the flow traces of ISOT dataset is used for training and testing purposes. Flow trace detection module is responsible to assemble a batch of flows two network endpoints. A flow trace is an ordered sequence of flows between two network endpoints. This module uses key < Source IP, DST Internet address, DST port, Protocol > to identify flows of two endpoints for the same application. flows with same key are grouped together to form a batch. Each flow of a batch is counted and when a batch reaches to the count of 10 flows that batch is exported to the feature extraction module. Any subsequent flow of the exported batch is recognized as a new trace and go

through the batch assembly process. The count of 10 flows is selected on bases of flow interval research in the literature which varies between a range of 10 to 60 flows. From trace source address or pointed to trace destination addresses in last 60-minute duration. The source and DST ADDR of the trace of interest are provided by feature extraction module. These addresses used as matching criteria to fetch flows from the controller. These flows are then forwarded to feature extraction module for further processing [6]. It Works with two time based separated batch of flows. The goal of this module is to extract statistical features from current network activity and historical context of the same. To achieve this two batch of flows are collected, first batch of 10 flows from trace detection module and second batch is collected from historical flow collection.

classification module uses C4.5 decision tree based supervised algorithm. The input to module is global feature vector generated by extraction It operates in two different modes. The system initially run in the training mode and the global feature vectors with pr-assign labeled to each fed into the classification module. C4.5 algorithm learn with help of provided labeled and create a decision tree model. This is then used in testing mode to detect botnet. Each input of feature vector during testing mode traverse through decision tree model and get assign a label. Real network traces for botnet and normal traffic are used to perform experiments. Six pcap files of different botnet families including Neris, Rbot, Virut, Menti, Murlou, and Sougo are collected and one pcap files for normal traffic [6]. Phase-1 for the training mode and phase-2 for the testing mode. The traffic for testing purposes has 50 percnent representation of unknown bot families for which the decision tree model is not trained. This is to test if proposed model can detect unknown botnet and to reduce dataset biasness. Experimental setup prepared using SDN controller opendaylight, the time series data repository (tsdr), the tsdr feature of opendaylight makes flow state collection abstract for user applications. The custom application only requires communicating with tsdr for collection of either flow stream or historical time series of flow stats. The prototype of the proposed system is developed in java. To simulate the dataset for evaluation, a network emulator tool called mininet is used to create Virtualized network infrastructure. This infrastructure is then used to simulate the dataset for training and testing purposes. Experiments are performed using labelled ground truth data and testing data. The results are compiled in two steps. The first step concludes the result at individual trace of interest granularity. This help to analyze system performance for individual botnet family sample included in testing

dataset. Three known botnet family samples and three unknown botnet family samples. The botnet samples including Rbot, Virut, and Menti are considered known botnet as detection model is trained for these whereas Neris, Murlo, and Soguo are considered as unknown botnet. The average detection rate of the proposed method for known botnet is 97.1 percent and for unknown botnet is 90.4 percent. The second step conclude results to analyze overall system performance. Overall accuracy of the proposed method is 94.8 percent. The paper concluded the proposed work detect botnet in software defined network in near real-time. The delay is approximately 10 consecutive flows counted from the first flow of a botnet trace. To increase detection rate and reduce false positives, the method uses a rich feature set extracted from current network activity of a trace and historical context of the same. The works shows promising results with detection rate of 97 percent for known and 90 percent for unknown botnet. The detection rate is much higher as compare to other approaches with same level of diversity in testing data. The proposed system shows accuracy of 94.8 percent. The system uses TSDR feature of opendaylight to support the concept of stats plan in SDNs. Separating statistics from control plan not only reduce computation load on controller but also provide a centralized statistics visibility. In context with stats plan, the future extension of this work is to reflects its computational results back to the stats plan so that other application may use this information [6].

It is important to discuss the performance of Bot-net detection by Neural Networks in SDN Same is done in paper [7]. It use Neural Networks to detect Bot-net in SDN. ANN classifier trained by available data sets collected in conventional networks. Accuracy of Bot-net detection higher than 99 percent.NN using the Kohonen algorithm trained to recognize unauthorized activities in a SDN. Managed from Open-daylight (ODL) controller in combination with Network Function Visualization (NFV) has been also proposed. It is based on a Self-Organized Map (SOM) learning method for the classification problem phase to build an IPS for DDoS attacks mitigation. The fundamental problem in NN-based botnet detection is the definition of suitable discriminators to detect malicious traffic against regular data in the network. Two hundred discriminators as the set of most Significant ones. A botnet classification strategy based on the centralized collection of network flow counters in SDN, and the use of a supervised C4.5 decision tree classification algorithm, is proposed. Analyzing only the Open-flow 1.3 messages exchanged. Traffic classification by an artificial neural network (ANN) to

identify Bot-nets in a SDN as playground. Such ANN is trained with a data training set (TS) obtained by a Bot-net attack running in conventional networks (CN), i.e. non SDN. Extracts a set of relevant parameters, referred to as discriminators. Supervised machine learning problem by using a Training Set (TS) and a Test Set with features computed from real traffic data with known malicious/non-malicious label. As features are numerical, we thought it was appropriate to use a Multilayer Perception (MLP), which is a classical and easily manageable ANN architecture, trainable with the error back-propagation weight update rule. Paper aimed to identify a small MLP that, after training, can be used as a real-time detection engine for Bot-nets. Determine the minimum number of hidden neurons in a MLP with a single layer that achieved an acceptable error rate. This preliminary study is particularly important for the Bot-net detection task. As a large number of neurons in the MLP results in longer computation time that may negatively affect the real-time performance of the desired detection engine. Paper found out that just 5 hidden sigmoid neurons were sufficient to achieve an acceptable error with a small improvement by using a higher number of hidden neurons. Consequently tried to increase the layers, just to discover a small improvement in the performance of Bot-net detection. kbDetector interactions with the SDN controller can be sketched as follows:- (i) The switch sends the Open-flow packet ofp in to SDN controller. (ii) replies to switch dictating to create a Flow Entry, and notifying, via Web-socket to kbDetector, that a new flow has started (iii) when hard-timeout expires, the switch sends a ofp flow removed Open-flow message with the statistics to the controller which then sends a notification via Web-socket to kbDetector that contains the statistics and the stream id. (iv) kbDetector calculates the features from incoming information and activates the trained MLP (v) If the MLP classifies flow as malicious, kbDetector retrieves the MAC address of the internal hosts involved in the flow and via REST messages add a block rule of flow in order to isolate the infected host in the appropriate SDN network switches flow entry. Developed the application kbTool, manages host blocked. Communicates via REST API with the controller in order to share configuration lies with kbDetector. Experiments for some selected MLP architectures that are reported for both CNs and SDN. All the MLP architectures were tested with different sizes of the time-window. main result we obtained is that an MLP trained over data concerning non-SDN has a very satisfactory performance also when tested for Bot-net detection in SDN. As expected, though, the test error in SDN is higher than that for non-SDN

they were trained for. Longer time windows bring about a better test error for most architectures, and that a four layers MLP is good enough to achieve an error rate of less than about 0.05percent. For experiments, paper compute features based on portions of packet trace until the layer 4 (ISO/OSIstack), thus the flows have same characteristics in SDN and CN, are completely transparent to an observer. The difference is in the specific set of discriminators used to train the ANN in two cases of CN and SDN. The MLP in experimentation were trained over a TS obtained by joining public datasets that are commonly used in the literature for Bot-net malicious traffic identification. The rest is CUT-13 dataset that come from different categories of Bot-nets. Then use the ISOT dataset [12] by taking out a small percentage of malicious traffic. Data-set have large number of flows in pcap (packet capture) format. Subdivision into small pcap files via Split-cap 3 for division of flows. ISOT dataset 9.9 GB contains 914812 different flows. Time windows: 10, 30, 60, 120, 180, 240, and 300 seconds. For each time window, 70percent of the files were used for the creation of the training set and the remaining 30 percent for the test set. New scenarios from the Stratosphere IPS 4 were added to the test set. training and test files have been splintered by duplicates. MLP was stopped either when the error was considered acceptable (0 percent) or when a maximum number of 1500 training epochs was reached. Performance of the trained MLP is measured by means of the confusion matrix with its four quadrants that represent TP, FP, TN and FN, Actual positives result $P = TP + FN$, Negatives $N = TN + FP$. Confusion matrix metrics resulting from are presented for the selected ANN architecture. The performance metrics for a supervised NN are computed from the four quadrants of the confusion matrix: the model accuracy is defined as $A = (TP + TN) / (P + N)$, Precision as $S = TP / (True\ positive + FP)$, and the recall as $Re = TP / P = TP / (TP + FN)$. The values of these performance metrics obtained in tests are shown vs. the time window's duration for both CN and SDN with protocol OpenFlow 1.3, for the selected ANN architecture. The experience of last October, when Mirai Botnet DDoS 17 Dyn Data Centers (DCs), repair sent a case study. Most dangerous threat for the performance of a DC is represented by a DDoS attack. Many cyber criminals started using the tool to assemble their own botnet armies. Paper simulated the same event in a SDN environment, by implementing a typical Fat-tree topology to create a Software-Defined Data Center (SDDC) with 4 pods within the Mininet framework. Simulator have infected with the Mirai malware six hosts in pods 1, 2 and 3, by listening on TCP ports 23 and

2323, in order to simulate vulnerable IoT web cams. One of the infected hosts plays the role of Mirai CnC server with a MySQL DBMS support, for scan receiver function used by Mirai. The victim host is located in pod 0, and undergoes two different DOS attacks: SYN Flood and UDP. Experimentation relies on the evaluation of the traffic flows in the network order to generate the set of relevant features to be given in input to the ANN for Bot-net detection. Evaluate the performance of approach in terms of confusion matrix metrics accuracy, recall and precision for Mirai detection. A sample of traffic between CnC and bots detected in a time window of 180 seconds. In particular, the packet set (in both directions) is represented by a quintuple consisting of source address, destination ADDR, SRC and DST PORT and protocol at the transport level. Paper analyze the efficiency of trained ANN as a Bot-net detection tool by simulating UDP flood attacks by bots replicated from the Mirai malware. Obtained the best performance in the attack detection for time windows of large duration, as expected, and for time windows of 240 or 300 seconds the performance is roughly the same. In practical implementations, the only possible time window with the current version 1.3 of OpenFlow protocol is 300 seconds. However, a real-time system for botnet detection would benefit significantly from the use of time-window sizes few seconds, Especially if measures, like, e.g., isolation from the rest of the network, should be taken. The main reason is that the current protocol is not provided with a method for extracting flow statistics at arbitrary time intervals, and the only way is by removing a flow entry from the switch. Furthermore, in a high traffic environment, such as DCs, that manage a large number of streams, it is mandatory to reduce of rule removals per second. So, there is no choice but setting the time window at the highest possible duration. Paper concluded by Statistical analysis and classification by a supervised neural network is an effective method for detecting the malicious traffic produced from bots during the attacks, for individuating the communication flow between bots and CnC for preventing the attacks. In addition, it have shown that it is possible to block the attacks at the source, not simply a mitigation strategy. During the testing phase we noticed, like a serendipity, that DDoS attacks were automatically recognized by neural network despite the work is explicitly focused on Bot-net detection and not on the application. In particular, the use of neural networks has been as effective as other Machine Learning methods with 99 percent accuracy. The use of OpenFlow protocol version 1.3 imposes some limits, like e.g., the impossibility of performing real-time detection, due to the constrained time

window duration. Future Work:- Open-flow 1.5.1 will be used, analysis of performance of the detection application by implementing the kbDetector with Big-Data techniques and the implementation of a malicious traffic generator to improve the results [7].

It is very important to get the knowledge of BOTNET definition, all BOTNETs classes that exists and can affect software defined networks. Paper discussed in [8] describe all type of BONET classifications available. Paper discussed that only few formal studies have examined the botnet problem and botnet research is still in its infancy. In this survey botnet detection techniques based on passive network traffic monitoring are classified into four classes including Signature-based Anomaly-based DNSbased Mining-base Signature-based techniques can only detect known botnets, whereas the other classes are able to detect unknown bots. However, most of the current botnet detection techniques work only on specific botnet CnC communication protocols and structures. According to the comparison, the most recent botnet detection techniques based on data mining as well as DNSbased botnet detection approach can detect real-world botnets regardless of botnet protocol and structure with a very low false positive rate. Hence, developing techniques based on data mining and DNS traffic for botnet CnC traffic detection has been the most promising approach to combat botnet threat against online ecosystems and computer assets [8].

Work done in [9] uses POX Controller, IPFIX template to detect bots, Offline analysis, Machine Learning approach, Categorization with Source IP, Destination IP, Ports, protocols, interface and class of service, number of packets, number of bytes, MLA used to detect bots, Flow collector, Multistage filtering to remove unnecessary data in five steps (i) detect IRC botnets (ii) Remove port scanning data (iii) remove high bit rate data flows (iv) remove flows with two or less packets, Botnet Detection Engine:- No MLA mentioned in the paper [9].

A research article [10] included in this document to get the idea of detecting point-to-point Botnet in Software defined networks. The solution use Machine Learning Approach. The captured packets with the same 5-tuple (i.e., source IP address, source port number, destination IP address, destination port number, and protocol) information and packets with reverse direction will be recognized as the same flow if they occur closely within a short time period. After a flow has been classified, the Detection Agent reports the result to the Rule Arbitrator with the 5-tuple information and the type of P2P botnet or application. The Rule Arbitrator, afterwards, modifies the related flowta-

bles in the Data-link Bridges in accordance with the result reported by the Detection Agent. Finally, the Data-link Bridges automatically drop the malicious packets that are recognized by the classifiers. It use Netmate, an open source tool, to capture packets and transform them into traffic flow, from which we extract feature vectors for machine learning analysis. This tool has been frequently used to capture network packets. Need to define the time frame to capture packets (i.e., a flow duration). Test different flow durations and analyze the performances. Based on the result, it found that the flow duration with 600 seconds has the best performance. Article propose a system which can detect and categorize P2P traffic in SDN with machine learning, automatically and flexibly adjust flow entries to manage network traffic, and thus reduce the load of network administrator. Experiment system in a test bed to evaluate the performance of classification accuracy and traffic management. Experiment results show that our system can detect all the considered types of P2P network traffic with high accuracy rate and automatically manage traffic with flow entries through SDN controller [10].

2.2 Limitation of Existing Techniques

The solution in this Paper is proposed after having a detailed literature survey to make sure that proposed technique covers all the limitations of existing technique with best possible method.

There are several limitations in technique proposed in [2], i.e. (i) Limited to OpenFlow protocol only (ii) Limited to only Open Daylight controller (iii) Only for known botnets 80 percent results accuracy (iv) Limited Publically available datasets Used (v) Only C4.5 Decision Tree used (vi) Feature extraction use feature set SP, DP, Protocol, Duration, Bytes, Packets, BPS, PPS, BPP, Pit (vii) Only detection is addressed not prevention (viii) Slow due to extensive computations for each flow (ix) Limited to specific types of botnets. Paper discussed in [5] is a survey paper, not reached to a single conclusion, limited to specific types of botnets and proposed only detection not prevention.

There are several limitations identified in paper given in [6] i.e. (i) A resource hungry process proposed as each time software have to identify 10 unique flows to form a single label, then search for 60minute traffic for this label. Then compare this label with last 60 minute traffic. (ii) Each time same process need to adapt and no record of successful detection given as feedback to the system for blocking without any further computation.

(iii) Only tested for open day light controller (iv) Only tested for OpenFlow (v) Only detection is addressed not prevention (vi) Limited to specific types of botnets. Solution proposed in Paper [9] is a resource hungry process as high computations involved, Multistage filtering again involve processing delay, Not real time, doing offline analysis, Only tested for POX controller, Only tested for IPFIX Templates, Only detection is addressed not prevention, Limited to specific types of botnets.

Paper in [7] has solution with resource hungry process proposed, each time same process need to adapt and no record of successful detection given as feedback to the system for blocking without any further computation. Only tested for specific controller. Only tested for OpenFlow 1.3. Analyzing only OpenFlow 1.3 messages exchanged. Use of non sdn networks for training data. What if new bot come in network? High time window required to get results. Higher error rate of proposed solution for SDN as compare to CN.

2.3 Chapter Summary

Literature survey is the most important part of any research to make sure that the proposed work is not done before and can cover the limitations of existing techniques. This chapter provides the detail of literature survey done for this Paper to make sure that proposed methodology caters the limitations and issues of existing techniques. First part of this chapter provides the detailed literature survey and then explained the limitations of existing techniques.

CHAPTER 3

Proposed Solution

This Paper proposed a DNS based approach to detect and prevent botnet by applying one million web database to software defined networks without reading packet payload. The proposed solution maintain good one million website database (1Mdb). To do any activity, Bot need to communicate with CnC and requires DNS to IP resolution. For any request having destination port 53 (DNS) will be checked. The protocol will get all matching traffic and send to 1Mdb. If URL Exists in 1Mdb then do not respond otherwise send reply with remove flow and block flow to the controller. The approach have a lot of benefits as compare to other approaches i.e. Very less computations on live traffic, Only Traffic for Port 53 will be monitored, No computation or processing on remaining traffic, Bots will be blocked at very start of communication, Infected IPs will be permanently blocked, System not only provide detection but also prevention solution, standard Technique for all type of controllers and protocols, isolate infected system before start of communication (Proposed solution architecture is shown in Figure-3.1 Below).

3.1 Proposed Solution Architecture Components

This section explains the architecture components that are used in the proposed solution and methodology.

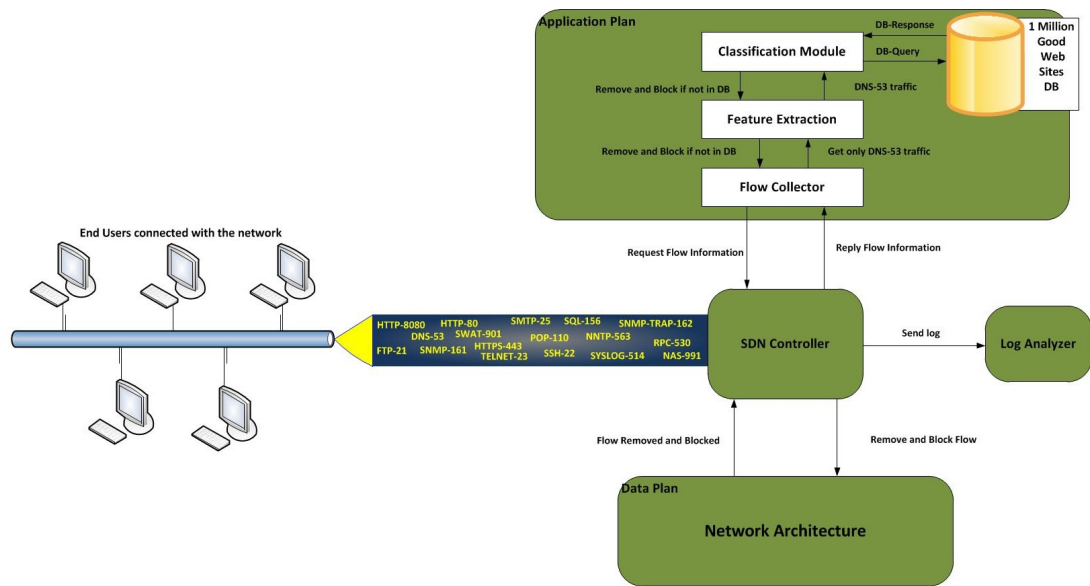


Figure 3.1: Proposed Solution Architecture Components

3.1.1 End User

End user is the part of solution architecture which is generating the user traffic and for which Bot detection will be processed.

3.1.2 SDN Controller

Controller is the heart of SDN network which control each and every packet to/from SDN networks. In the propose solution, the open day light controller has been used. The controller is used to extract the required feature set by flow request and to block/remove flow as per decision done by application plan.

3.1.3 Flow Collector

Feature collector module is one of the most important module of the proposed solution. This module have to collect each and every packet of the network with all header information. The module will cover all protocols to collect form each part of the Software Defined Network via Controller to make sure that all traffic passed to the proposed solution for further processing. As this module have to process huge amount of data so it must be very accurate and fast to avoid any packet loss. After processing at its end, this module will forward traffic to feature extractor module for further processing.

3.1.4 Feature Extractor

Feature extractor module will collect the selected features from all the flows coming from flow collector. In our case only dns traffic on port 53 will be extracted. The source IP address, destination protocol, destination service and destination URL will be extracted as feature set.

3.1.5 Classification Module

The classification module will classify either the URL is a legitimate website or related to CnC botnet traffic. For this the classification module query from the one million good website database. If the answer found yes then it will classify it as legitimate and no action will be taken otherwise the flow will be considered as bot-traffic and will be blocked and removed. Naive Bayes Classifier can be used to classify the data.

3.1.6 One Million Good Websites database

A one million database has been used in the proposed solution to cross check each dns request from one million good website database. If the requested url exists in this database then no further action need to be taken otherwise respective flow will be removed and blocked for further communication. This database is available to download from <http://s3-us-west-1.amazonaws.com/umbrella-static/index.html> and is regularly updated.

3.1.7 Log Analyzer

Log analyzer has been added in the proposed solution to keep log of each flow that has been removed or blocked from the network to keep track of traffic that is not passing from the network.

3.1.8 Dataset

The selection of dataset is very important task for machine learning based botnet detection and prevention techniques. The poor selection of dataset possibly lead to biased results. The real world and publically available dataset is a good choice for evaluation

of botnet detection techniques. To meet these criteria, we will use publicly available CTU-43 botnet dataset. This dataset provide packet dumps (pcap files) of seven real botnets (Neris, Rbot, Virut, Murlo, Menti, Sogou, and NSIS). We will use these files to generate botnet traffic for evaluation and test our model. To generate normal traffic, we selected ISOT dataset. This dataset provides a single pcap file having normal traffic and traffic for weladec and zeus botnet. Other dataset includes the one million website datasets as well. Brief detail of these datasets are given below:-

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_db:19:c3	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.1
2	8.982709	Cisco_db:19:c3	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.1
3	50.099564	Cisco_db:19:c3	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.1
4	50.369266	54:52:00:00:00:01	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.85
5	51.369054	54:52:00:00:00:01	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.85
6	52.369688	54:52:00:00:00:01	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.85
7	53.086840	Cisco_db:19:c3	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.1
8	59.086131	Cisco_db:19:c3	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.1
9	160.084662	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
10	160.084668	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
11	161.077511	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
12	161.077519	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
13	162.079007	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
14	162.079013	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
15	162.765245	147.32.84.165	147.32.84.255	NBNS	110	Registration NB SARUMAN<00>
16	162.765253	147.32.84.165	147.32.84.255	NBNS	110	Registration NB SARUMAN<00>
17	163.510681	147.32.84.165	147.32.84.255	NBNS	110	Registration NB SARUMAN<00>
18	163.510692	147.32.84.165	147.32.84.255	NBNS	110	Registration NB SARUMAN<00>
19	163.926344	PcsCompu_b5:b7:19	Broadcast	ARP	60	Who has 147.32.84.1? Tell 147.32.84.165
20	163.926354	PcsCompu_b5:b7:19	Broadcast	ARP	60	Who has 147.32.84.1? Tell 147.32.84.165
21	163.929830	Cisco_db:19:c3	PcsCompu_b5:b7:19	ARP	60	147.32.84.1 is at 00:1e:49:db:19:c3

Figure 3.2: CTU-43 Dataset

No.	Time	Source	Destination	Protocol	Length	Info
1824317	162035673.303591	188.72.243.72	172.16.2.12	TCP	1434	[TCP segment of a reassembled PDU]
1824318	162035673.303719	172.16.2.12	188.72.243.72	TCP	60	1035→80 [ACK] Seq=168 Ack=586501 Win=64860 Len=0
1824319	162035673.303903	188.72.243.72	172.16.2.12	TCP	1434	[TCP segment of a reassembled PDU]
1824320	162035673.304076	172.16.2.12	188.72.243.72	TCP	60	1035→80 [ACK] Seq=168 Ack=589261 Win=64860 Len=0
1824321	162035673.304418	188.72.243.72	172.16.2.12	TCP	1434	[TCP segment of a reassembled PDU]
1824322	162035673.304502	188.72.243.72	172.16.2.12	TCP	1434	[TCP segment of a reassembled PDU]
1824323	162035673.304634	172.16.2.12	188.72.243.72	TCP	60	1035→80 [ACK] Seq=168 Ack=590641 Win=64860 Len=0

▶ Frame 1824317: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface 0
 ▶ Ethernet II, Src: cc:cc:cc:cc:cc:cc (cc:cc:cc:cc:cc:cc), Dst: cc:cc:cc:cc:cc:cc (cc:cc:cc:cc:cc:cc)
 ▶ Internet Protocol Version 4, Src: 188.72.243.72, Dst: 172.16.2.12
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 1035, Seq: 586501, Ack: 168, Len: 1380

```

0000  cc cc cc cc cc cc cc cc cc cc cc cc cc 08 00 45 00  .....l.
0010  05 8c 17 dd 40 00 35 06 b5 14 bc 48 f3 48 ac 10  ...@.5. ...H.H..
0020  02 0c 00 50 04 0b e5 4b dc 4b ec 9d f5 85 50 10  ...P...K .K....P.
0030  19 20 ef 6c 00 00 55 48 55 76 51 6b 68 69 59 33  . .1..UH UvQkhIY3
0040  49 30 51 6a 49 7a 56 55 68 70 0d 0a 65 44 5a 45  IQQjIzVU hp..eDZE
0050  4e 33 5a 33 55 6a 4a 34 53 45 70 42 5a 48 52 36  N3Z3UjJ4 SEp0ZHR6
  
```

Packets: 1824341 · Displayed: 1824341 (100.0%) · Load time: 0:25.580 · Profile: Default

Figure 3.3: ISOT Dataset

SN	Website
1	netflix.com
2	api-global.netflix.com
3	prod.netflix.com
4	push.prod.netflix.com
5	google.com
6	www.google.com
7	microsoft.com
8	doubleclick.net
9	g.doubleclick.net
10	safebrowsing.googleapis.com
11	facebook.com
12	ichnaea.netflix.com
13	googleads.g.doubleclick.net
14	google-analytics.com
15	clients4.google.com
16	data.microsoft.com
17	live.com
18	apple.com
19	clientservices.googleapis.com

Figure 3.4: One Million DB Dataset

3.2 Comparison

A brief comparison of existing solutions and proposed one is given below:-

Referen ce	Header + Data	Ana lyze each pack et	Com ple x	Perf orm ance	Approach	Stand ardize d for all Contr ollers	Algori thm	Proto cols Analy zed	Blocking of BOTs	Protec tion
DISCLOS URE[2]	Header only	Yes	Yes	Slow	Machine Learning	No	C 4.5	All	During or after communication	Detecti on Only
DISCLOS URE[5]	Header + Body	Yes	Yes	Slow	Honeypot	No	Honey pot	All	During or after communication	Detecti on Only
DISCLOS URE[6]	Header only	yes	Yes	Slow	Machine Learning	No	C 4.5	All	During or after communication	Detecti on Only
DISCLOS URE[7]		Yes	Yes	Slow	Neural Net classier	No	Kohon en algorit hm C4.5	All	During or after communication	Detecti on Only
Proposed Solution	Header Only	No	No	Fast	Machine Learning	Yes	Naive Bayes Classi fier	DNS only	Before Start of any communication	Detecti on and Preventi on

Figure 3.5: Comparison

CHAPTER 4

Methodology, Implementation and Results

4.1 Deployment and Implementation

4.1.1 Flow Chart

Flow chart is given in this sub-section to explain the exact process flow for proposed solution. Same flow has been adopted to implement the system. User data will first reach to controller via control plan of Software Defined network. The data then will be collected by flow collector and will send to packet filter only for DNS traffic on destination port 53. All DNS traffic will be matched with 1Million good web sites database. If destination URL found in 1Mdb then no action will be taken otherwise flow will be forwarded to data plan for further necessary action to block and remove the flow and all its associated traffic. Flow chart is given below.

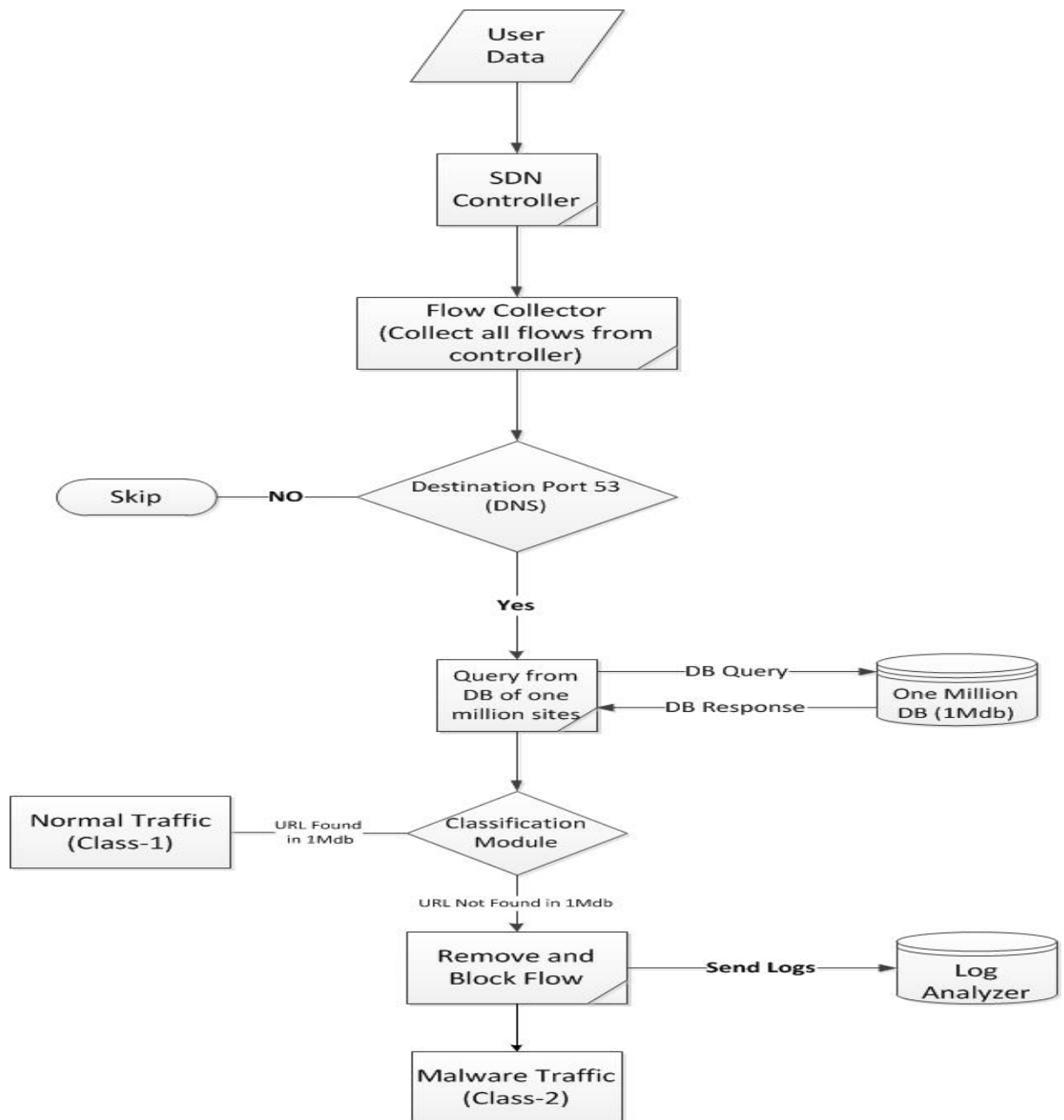


Figure 4.1: Flow Chart

4.1.2 Implementation

The implementation of the proposed solution will be performed by using python programming language. All the datasets will be imported to verify the traffic and to take appropriate decisions on the results.

4.1.3 Algorithm

Before implementation the program in the python programming language, an algorithm has been written so that same steps can be reflected in the code.

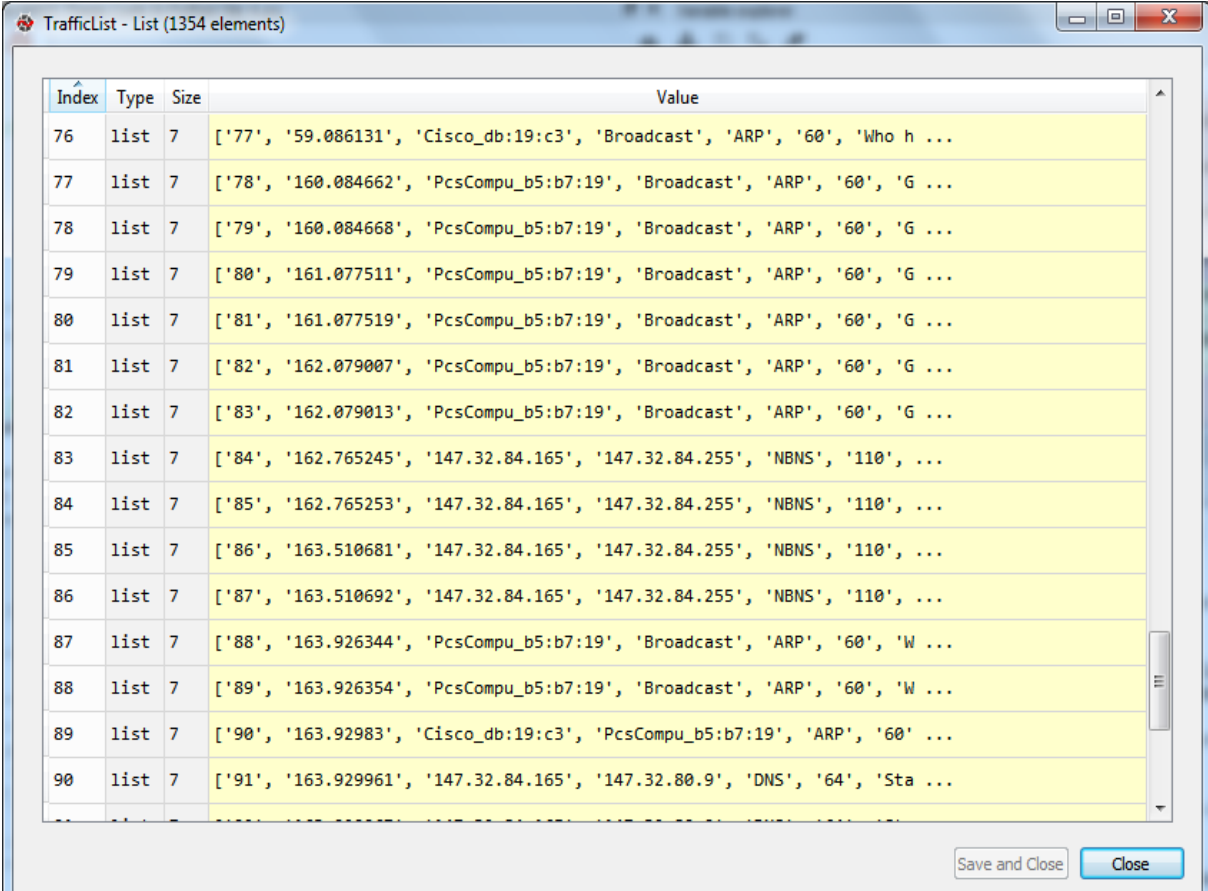
1. Import required libraries
2. Import 1Mdb datasets
3. Import Malware datasets
4. Import normal traffic datasets
5. Apply filter on destination port 53
6. If destination port = 53 then query the destination URL from 1Mdb else no action
7. If URL found in 1Mdb then no action required and mark traffic as Normal Traffic (Class-1)
8. If URL not found in 1Mdb then remove and block flow from data plan, send log to log analyzer and Mark traffic as Malware Traffic (Class-2).

4.2 Results

This section provide the results that are computed via program written in python language. Output of each step has been given in each subsection below then concluded on the final output of the program with the classification of user traffic.

4.2.1 Traffic List

All traffic data has been imported by using datasets mentioned in previous sections. Below is the sample import snap of dataset taken from the output of python program:-

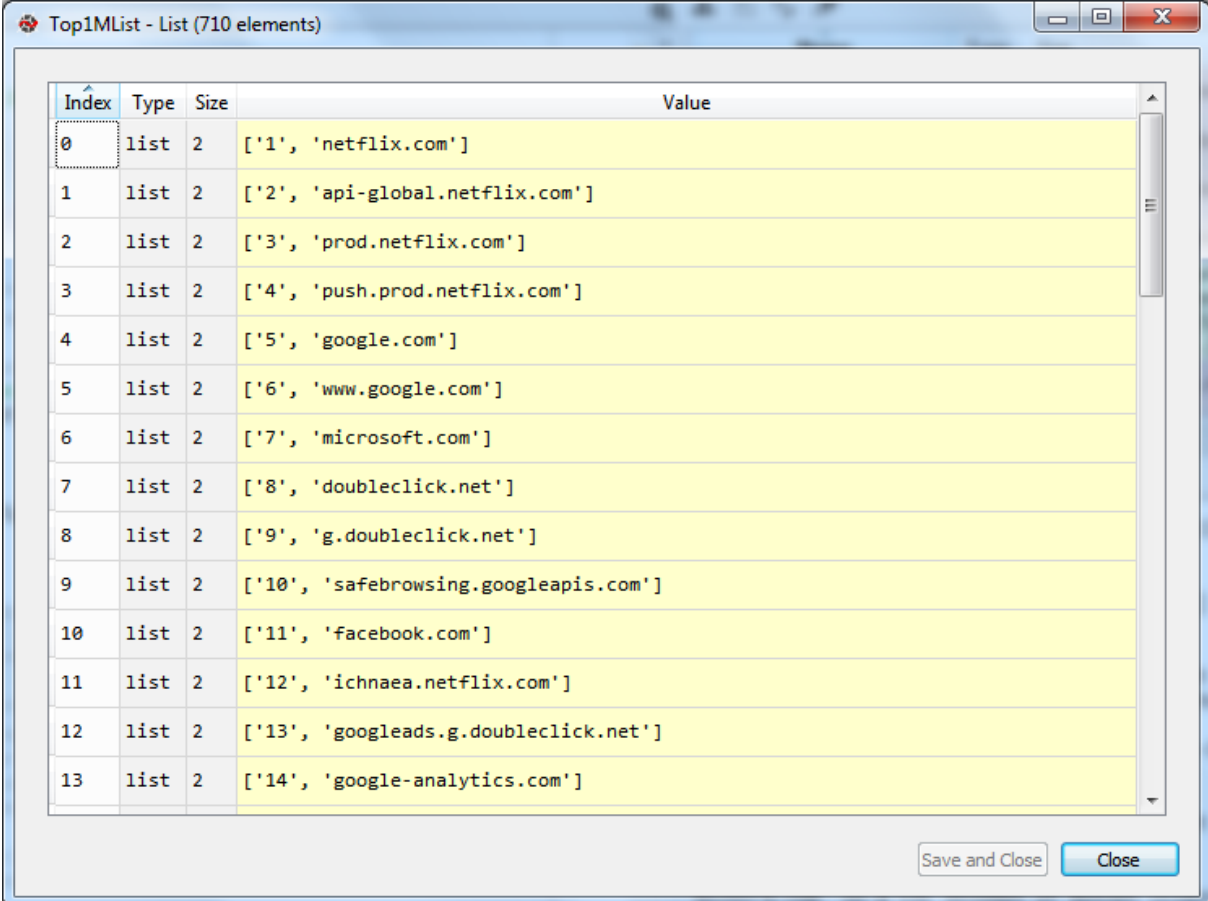


Index	Type	Size	Value
76	list	7	['77', '59.086131', 'Cisco_db:19:c3', 'Broadcast', 'ARP', '60', 'Who h ...
77	list	7	['78', '160.084662', 'PcsCompu_b5:b7:19', 'Broadcast', 'ARP', '60', 'G ...
78	list	7	['79', '160.084668', 'PcsCompu_b5:b7:19', 'Broadcast', 'ARP', '60', 'G ...
79	list	7	['80', '161.077511', 'PcsCompu_b5:b7:19', 'Broadcast', 'ARP', '60', 'G ...
80	list	7	['81', '161.077519', 'PcsCompu_b5:b7:19', 'Broadcast', 'ARP', '60', 'G ...
81	list	7	['82', '162.079007', 'PcsCompu_b5:b7:19', 'Broadcast', 'ARP', '60', 'G ...
82	list	7	['83', '162.079013', 'PcsCompu_b5:b7:19', 'Broadcast', 'ARP', '60', 'G ...
83	list	7	['84', '162.765245', '147.32.84.165', '147.32.84.255', 'NBNS', '110', ...
84	list	7	['85', '162.765253', '147.32.84.165', '147.32.84.255', 'NBNS', '110', ...
85	list	7	['86', '163.510681', '147.32.84.165', '147.32.84.255', 'NBNS', '110', ...
86	list	7	['87', '163.510692', '147.32.84.165', '147.32.84.255', 'NBNS', '110', ...
87	list	7	['88', '163.926344', 'PcsCompu_b5:b7:19', 'Broadcast', 'ARP', '60', 'W ...
88	list	7	['89', '163.926354', 'PcsCompu_b5:b7:19', 'Broadcast', 'ARP', '60', 'W ...
89	list	7	['90', '163.92983', 'Cisco_db:19:c3', 'PcsCompu_b5:b7:19', 'ARP', '60' ...
90	list	7	['91', '163.929961', '147.32.84.165', '147.32.80.9', 'DNS', '64', 'Sta ...

Figure 4.2: Actual User Traffic

4.2.2 Top One Million Web Site Database

Top one million web site database has been imported by using the authentic data as mentioned in the dataset section of this document. Below is the sample import snap of dataset taken from the output of python program:-

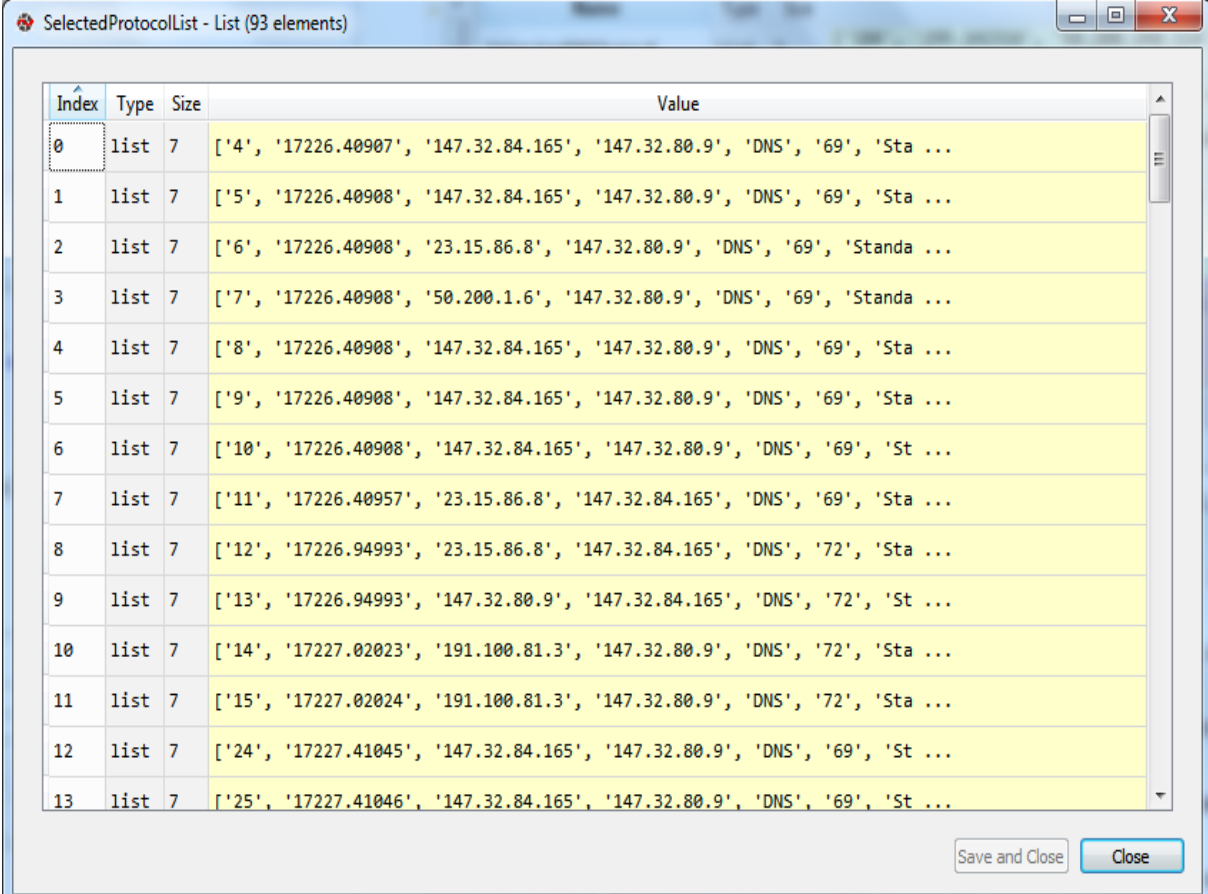


Index	Type	Size	Value
0	list	2	['1', 'netflix.com']
1	list	2	['2', 'api-global.netflix.com']
2	list	2	['3', 'prod.netflix.com']
3	list	2	['4', 'push.prod.netflix.com']
4	list	2	['5', 'google.com']
5	list	2	['6', 'www.google.com']
6	list	2	['7', 'microsoft.com']
7	list	2	['8', 'doubleclick.net']
8	list	2	['9', 'g.doubleclick.net']
9	list	2	['10', 'safebrowsing.googleapis.com']
10	list	2	['11', 'facebook.com']
11	list	2	['12', 'ichnaea.netflix.com']
12	list	2	['13', 'googleads.g.doubleclick.net']
13	list	2	['14', 'google-analytics.com']

Figure 4.3: Top One Million Database

4.2.3 Selected Protocol List

User traffic then filtered by using feature extraction module. As the algorithm is based on the filtration of user traffic on DNS protocol. So after filtration, only DNS traffic will remain to be processed for next step. Below is the sample output of feature extraction step that is taken from the output of python program:-

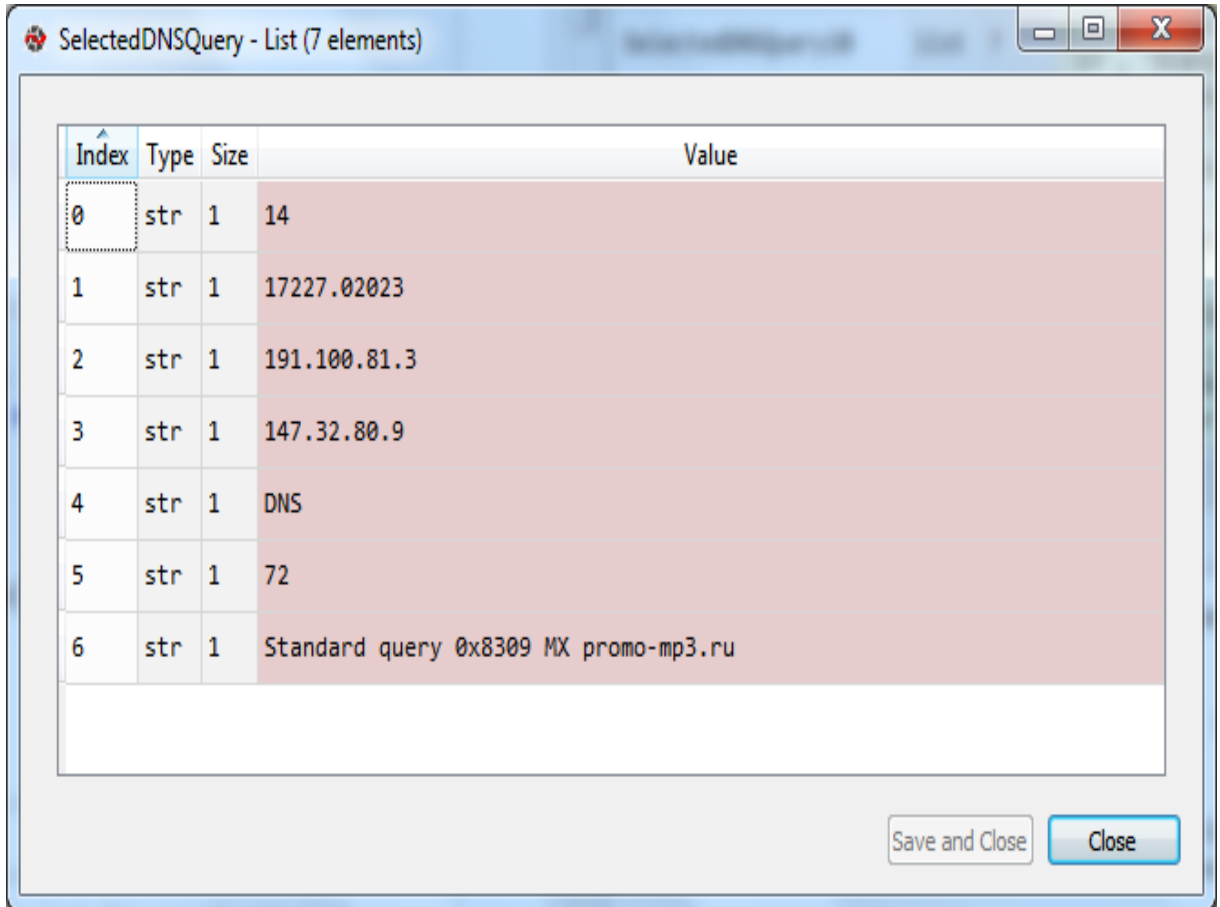


Index	Type	Size	Value
0	list	7	['4', '17226.40907', '147.32.84.165', '147.32.80.9', 'DNS', '69', 'Sta ...
1	list	7	['5', '17226.40908', '147.32.84.165', '147.32.80.9', 'DNS', '69', 'Sta ...
2	list	7	['6', '17226.40908', '23.15.86.8', '147.32.80.9', 'DNS', '69', 'Standa ...
3	list	7	['7', '17226.40908', '50.200.1.6', '147.32.80.9', 'DNS', '69', 'Standa ...
4	list	7	['8', '17226.40908', '147.32.84.165', '147.32.80.9', 'DNS', '69', 'Sta ...
5	list	7	['9', '17226.40908', '147.32.84.165', '147.32.80.9', 'DNS', '69', 'Sta ...
6	list	7	['10', '17226.40908', '147.32.84.165', '147.32.80.9', 'DNS', '69', 'St ...
7	list	7	['11', '17226.40957', '23.15.86.8', '147.32.84.165', 'DNS', '69', 'Sta ...
8	list	7	['12', '17226.94993', '23.15.86.8', '147.32.84.165', 'DNS', '72', 'Sta ...
9	list	7	['13', '17226.94993', '147.32.80.9', '147.32.84.165', 'DNS', '72', 'St ...
10	list	7	['14', '17227.02023', '191.100.81.3', '147.32.80.9', 'DNS', '72', 'Sta ...
11	list	7	['15', '17227.02024', '191.100.81.3', '147.32.80.9', 'DNS', '72', 'Sta ...
12	list	7	['24', '17227.41045', '147.32.84.165', '147.32.80.9', 'DNS', '69', 'St ...
13	list	7	['25', '17227.41046', '147.32.84.165', '147.32.80.9', 'DNS', '69', 'St ...

Figure 4.4: Selected Protocol List

4.2.4 DNS Query

Below is the snap of single DNS query having source IP, DNS Server IP, Protocol and the URL that is required to be accessed by end user:-



The screenshot shows a window titled "SelectedDNSQuery - List (7 elements)". Inside the window is a table with 4 columns: Index, Type, Size, and Value. The table contains 7 rows of data. The first row (Index 0) has a Type of "str", Size of 1, and Value of 14. The second row (Index 1) has a Type of "str", Size of 1, and Value of 17227.02023. The third row (Index 2) has a Type of "str", Size of 1, and Value of 191.100.81.3. The fourth row (Index 3) has a Type of "str", Size of 1, and Value of 147.32.80.9. The fifth row (Index 4) has a Type of "str", Size of 1, and Value of DNS. The sixth row (Index 5) has a Type of "str", Size of 1, and Value of 72. The seventh row (Index 6) has a Type of "str", Size of 1, and Value of Standard query 0x8309 MX promo-mp3.ru. At the bottom right of the window are two buttons: "Save and Close" and "Close".

Index	Type	Size	Value
0	str	1	14
1	str	1	17227.02023
2	str	1	191.100.81.3
3	str	1	147.32.80.9
4	str	1	DNS
5	str	1	72
6	str	1	Standard query 0x8309 MX promo-mp3.ru

Figure 4.5: A DNS Query

4.2.5 Results

This section shows that results that is provided by the Classification module which classified that either the traffic is a BOTNET CnC traffic or legitimate traffic. Results are given below:-

promo-mp3.ru is Clean Traffic not CnC [Class-1] Source IP: 191.100.81.3 Destination IP: 147.32.80.9 Destination Protocol: DNS

thiswebonline.com is a CnC Attempt of Botnet [Class-2] Source IP: 147.32.80.9 Destination IP: 147.32.80.9 Destination Protocol: DNS

irc.zief.pl is a CnC Attempt of Botnet [Class-2] Source IP: 147.32.84.165 Destination IP: 147.32.80.9 Destination Protocol: DNS

dns4.zief.pl is a CnC Attempt of Botnet [Class-2] Source IP: 147.32.80.9 Destination IP: 147.32.80.9 Destination Protocol: DNS

ii.ebatmoyhuy.com is a CnC Attempt of Botnet [Class-2] Source IP: 54.208.248.114 Destination IP: 147.32.80.9 Destination Protocol: DNS

accessonline-dlbtransfer.com is a CnC Attempt of Botnet [Class-2] Source IP: 147.32.84.165 Destination IP: 147.32.80.9 Destination Protocol: DNS

api.iris.microsoft.com is Clean Traffic not CnC [Class-1] Source IP: 23.15.86.8 Destination IP: 147.32.80.9 Destination Protocol: DNS

aduidc.xyz is a CnC Attempt of Botnet [Class-2] Source IP: 221.154.7.98 Destination IP: 147.32.80.9 Destination Protocol: DNS

pippio.com is Clean Traffic not CnC [Class-1] Source IP: 50.200.1.6 Destination IP: 147.32.80.9 Destination Protocol: DNS

soluxury.co.uk is a CnC Attempt of Botnet [Class-2] Source IP: 201.232.100.96 Destination IP: 147.32.80.9 Destination Protocol: DNS

hotjar.com is Clean Traffic not CnC [Class-1] Source IP: 147.32.84.165 Destination IP: 147.32.80.9 Destination Protocol: DNS

people-pa.googleapis.com is Clean Traffic not CnC [Class-1] Source IP: 147.32.84.165 Destination IP: 147.32.80.9 Destination Protocol: DNS

l.betrad.com is Clean Traffic not CnC [Class-1] Source IP: 147.32.84.165 Destination IP: 147.32.80.9 Destination Protocol: DNS

specialistups.com is a CnC Attempt of Botnet [Class-2] Source IP: 91.200.4.8 Destination IP: 147.32.80.9 Destination Protocol: DNS

mulbora.com is a CnC Attempt of Botnet [Class-2] Source IP: 100.50.64.98 Destination IP: 147.32.80.9 Destination Protocol: DNS

Accuracy of the proposed solution has been calculated using following formula

Accuracy =

$$\frac{TP + TN}{TP + TN + FP + FN}$$

All the datasets were passed from the algorithm to find out the accuracy of our detection and prevention model. Results shows 83 Percent accuracy.

4.3 Future Work

For future work, the model that has been proposed in this Paper can be used further with other Machine learning algorithms and protocols as well to check the accuracy and performance of proposed solution with all available options.

References

- [1] Ayesha Imran, (2017). SDN Controller Security Issues. University of Jyväskylä, Department of Mathematical Information Technology.
- [2] Tariq, F., Baig, S. (2016). Botnet classification using centralized collection of network flow counters in software defined networks. *International Journal of Computer Science and Information Security*, 14(8), 1075.
- [3] Bilge, L., Balzarotti, D., Robertson, W., Kirda, E., Kruegel, C. (2012, December). Disclosure: detecting botnet command and control servers through large-scale net-flow analysis. In *Proceedings of the 28th Annual Computer Security Applications Conference* (pp. 129-138). ACM.
- [4] Stevanovic, M., Pedersen, J. M. (2014, February). An efficient flow-based botnet detection using supervised machine learning. In *2014 international conference on computing, networking and communications (ICNC)* (pp. 797-801). IEEE.
- [5] Hadiano, R., Purboyo, T. W. (2018). A Survey Paper on Botnet Attacks and Defenses in Software Defined Networking. *International Journal of Applied Engineering Research*, 13(1), 483-489.
- [6] Tariq, F. Baig, S. (2017). Machine learning based botnet detection in software defined networks. *International Journal of Security and Its Applications*, 11(11), 1-11.
- [7] Letteri, I., Del Rosso, M., Caianiello, P., Cassioli, D. (2018). Performance of Botnet Detection by Neural Networks in Software-Defined Networks. In *ITASEC*
- [8] Feily, M., Shahrestani, A., Ramadass, S. (2009, June). A survey of botnet and botnet detection. In *2009 Third International Conference on Emerging Security Information, Systems and Technologies* (pp. 268-273). IEEE.

- [9] Wijesinghe, U., Tupakula, U., Varadharajan, V. (2015, January). An enhanced model for network flow based botnet detection. In Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015) (Vol. 27, p. 30).
- [10] Su, S. C., Chen, Y. R., Tsai, S. C., Lin, Y. B. (2018). Detecting p2p botnet in software defined networks. Security and Communication Networks, 2018.

An Improved Approach for Monitoring and Controlling of Flyovers And Bridges Using Internet of Things

K. S. F. Azam ^{1*}, D. M. Abdullah ², Md. M. Rahman ³, Md.S.Bari ⁴

¹ Department of Computer Science & Engineering, Primeasia University, Dhaka, Bangladesh.

² Department of Computer Science & Engineering, Primeasia University, Dhaka, Bangladesh.

³ Department of Computer Science & Engineering, Primeasia University, Dhaka, Bangladesh.

⁴ Department of Computer Science & Engineering, Primeasia University, Dhaka, Bangladesh.

e-mail: tahia.pau@gmail.com, deen.abdullah@primeasia.edu.bd, moshur.pau@gmail.com, sadikulbari2209@gmail.com

*Corresponding Author: tahia.pau@gmail.com, Tel.: +880-1982897386

Abstract—In modern technology robotics method may be applied to do our manual task. If robots are to become as common at household people will need to control and monitor them easily. In this aspect we have proposed, desired and designed a robot which can be controlled by mobile phones. Through which we can call for some emergency situations for Fire brigade, Law enforcement agency (Police, Army), Natural Calamity, Area Guard so on. On Mobile phone robot we have mounted a 9V battery as the power supply for the circuit and the motors. When the user calls the mobile the call is received by auto-answer mode. As the call continues when the user presses a button on his handset the tone that is generated is decoded by the DTMF decoder and the command is passed to the microcontroller which is pre-programmed. The Microcontroller then passes the command to the motor driver ICs for motion. It can also be used in reconnaissance or surveillance and anywhere there is the service provider tower of the connection provided that is mounted on the robot and Mostly The robot is small in size and its cost is also reasonable.

Keywords— DTMF (Dual Tone Multiple Frequency) Board (MT8870), Mobile phone, Microcontroller, Dc motor, Motor Driver (L293D), Crystal (3.57MHz), 7805 IC, Robot Chassis, DC power Supply.

I. INTRODUCTION

Every now and then ground breaking innovations are taking place in robotics field. Different types of robotic state of arts have taken place in 20th century. Aiming to assist more and more to the different human functions; robotics are an accumulative instrument for practical life.

Versatility, ingenious and accustomed with professional environment are fit with human beings whereas a robot is stand for humans to assist different tasks which are required to perform more sensible and on edge.

Mobile controlled robot is a programmed machine which is inclined of assurance. Such as an example, a spying robot being controlled by mobile whose movements are directed by users provided direction. They are flexible to work in different locations and can serve around where user wants. These mobile controlled robots are commanded from an user end through a mobile phone. Within their power available areas; mobile robots are adjusted for seizing, grasping, or taking hold of something which can terminologies as their "Independence".

Mobile Robot consists of different types of major components such as a controller with application or

software's, DTMF board, actuators and sensors. Generally controller in consist by a microprocessor which rooted with microcontroller. Above mentioned controller with its application or software written by primary or high level languages. Most used languages are C, C++, Fortan, Pascal and so on. Applied sensors in the mobile robot are dependent upon robots requirement and requirements are defined as proximity sensor to identify nearby objects, triangulation ranging for determination of location of a point, collision warning system by using radar or laser, dead reckoning functions to figuring out first starting point by using speed; direction & time and other specific application and methods which is discussed in section III.

II. RELATED WORK

Related works have been done in different sectors and places such as industrial, pharmaceutical, environmental and services robots are available. To enhance industrial manufacturing and improve the quality; industrial robots are being used. In this sector robots are developed for such application as connecting or joining, transferring materials, brushes something and other works. Sensitive but limited

tasks are being handled by robots in medicine and medical sector. Even now a day some surgeries are also being done by robots. The broadest category is entertainment sector where robots are holds a vast position. Form the Robosapien to Running Alarm Clock everything are being considered as entertainment robot. Also weight lifting robots are also considered as articulated robot.

Due to having a huge contribution in economic sectors above mentioned mobile applications are now accessible for further development. Although Entertainment industry makes a massive difference then others. They have a huge contribution in economic sector. Due to automated inspection it's developed its own economic importance.

Due to heavy costly inspection in manual process due to operate by a human operator, it's also grow risks as well.

Now a day, restaurants are also using robots as a cook and to serve food. China also implemented 18 types of restaurants with robots where they are cooking and serving to customers. Dumpling and Noodle robots are also using for serving dishes. Abovementioned robots are manufactured by local companies and definitely directed from remote area. [4]

The Famous car manufacturing company Ford Motor using 92 robots in their Indian factory. The programs of these robots are sourced consecutively from ABB Company; Sweden and DURR company in Germany. Due to fulfill the gradual demand, cost efficiency, cutting edge quality and flexibility; Ford India company imported those robots. [5]

To reduce the cleaning cost, robots are also used in different offices also. Cleaning robots can automatically organize their tasks without consuming extra energy. From all types of energy and financial consumption, cleaning robots are well performed and proved as cost efficient products. [9]

III. METHODOLOGY

A. System Design:

The project aims to design a Robot that can be moved using mobile phones when button is pressed. Warless controlled functionality is used to move the robot through mobile phone. Using mobile networks, mobile phone is used as a remote controller to operate the robot. A DTMF Board and DC motor is interfaced with the Microcontroller and the Microcontroller is the key part of the device who control the whole system. After sending the signal from a mobile through a mobile network, data received by the DTMF Board. It was fed while it pressed; to make an input to the controller. To realize and accomplish the task the controller is sourced with a specified written program coded by 'C' language. Fig in 1.

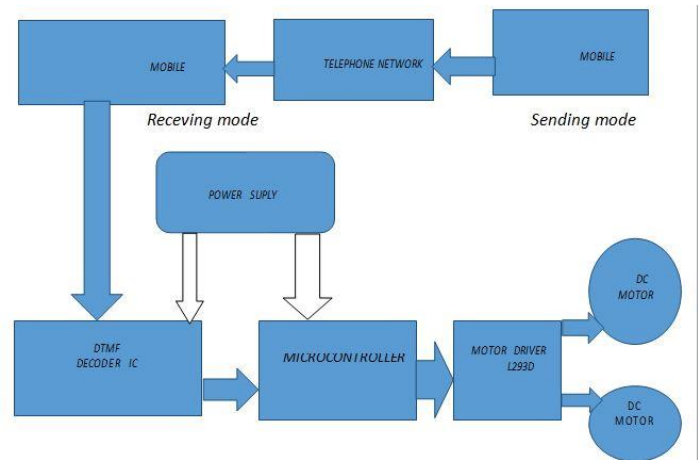


Figure 1: Block diagram of the mobile controlling robot

The model is organized based on a very simple and understandable working procedure. Firstly, turn ON of the robot needs with the power supply of 9v battery. Mobile number should be dialed which is connected to robot at remote location to move. Then the mobile automatically connected by Auto Answer option in mobile phone as like as two systems to operate. It needs to be ensured that DTMF tones sending facility should be active between both mobiles for working the robot in desired way. After connection it is able to operate the robot using the keyboard in particular direction for making a process successful. Flow chart of the whole circuit is very helpful for perceiving the working principle of the given model. For that purpose the operational flow chart is shown in fig 2.

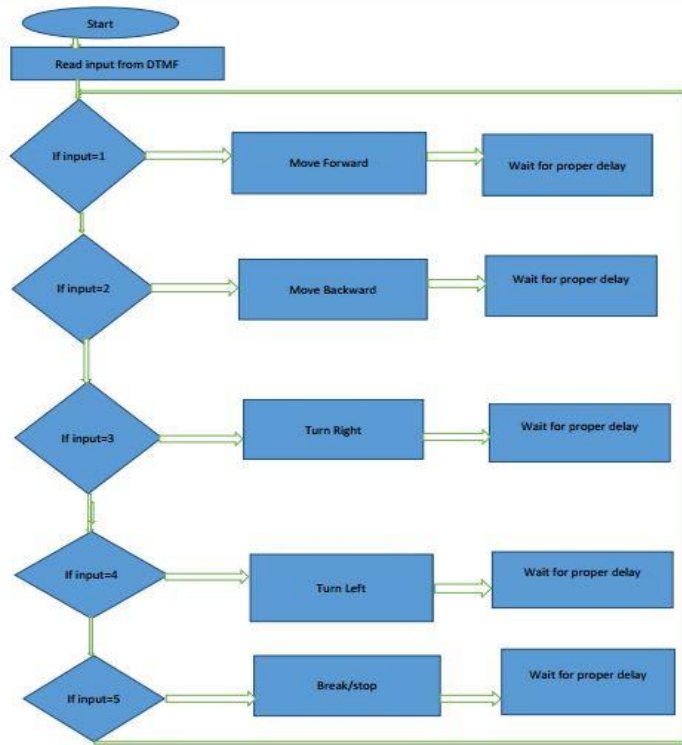


Figure 2: Coding flow chart

B. Sytem Setup:

The main purpose of this project was to build a communication between two mobile phones and provide the ability to operate the robot physically from a remote location. This purpose is suitable for the places where mobile phone use is available for making the transaction easier to easier. The device is responsible for including two interface systems. One of these interface is answerable between actuators and a transmitting mobile phone, and the rest interface is liable between the receiving mobile phone and the robot device. The interface on the transmitting side would allow occurrence and encipher of signals appropriate for transmission via a mobile device. The interface on the receiving side would action the signals acknowledged by the mobile phone and regulate the robot device. The simple diagram illustrates the methodology of the project below in fig 3.

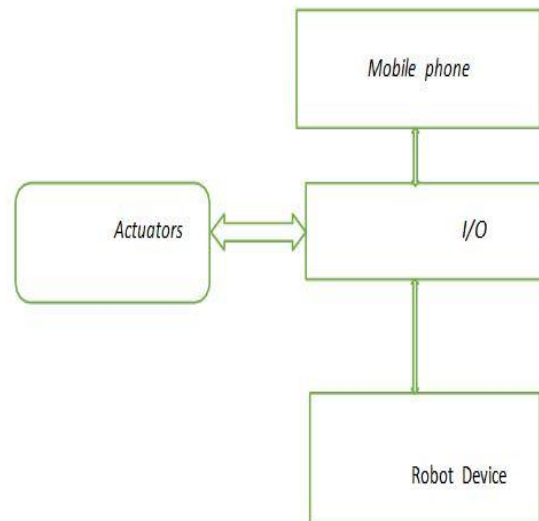


Figure 3: user interface of mobile controlling robot

C. Robot Vision:

Worked with our project for an hour in a room which was around 1100 sq. ft.our vision was searching the different object through our device and we started with few different object places in different corner of the room .we moved the robot from an initial point and kept a mobile phone attached with the device to connect with the robot from another phone. Then we controlled it to search those object from the starting point as our requirements. In addition we tried also to control it from different room and different spaces. While doing the experiment we cared about measurement of such things like as call cost, internet data, voltage power, time of searching and so on.

After the observation it was cleared that during any disaster with this robot will be possible to communicate with any location remotely.

IV. IMPLEMENTATION

The DTMF (Duel Tone Multiplexed Frequency) is the identical tones for different keys of the dial pad. When someone calls either in telephone or mobile, a keypad input can generate this DTMF tone. From this tone, key number can be identified.

Anyway, there is an IC that can detect this DTMF tone and decode the key number from tone. IC is MT8870 DTMF decoder. This decoder takes input from audio output of a cell phone. Then it decodes the tone and gives output in BCD (binary coded decimal) value.

Here in our project, we used a microcontroller PIC16F73B to work with. We are reading that BCD code from MT8870 and then doing rest of the work from that command. MT8870 has 4 output pins connected with 4pins of PORTA,

MCU is reading this 4pins of PORTA. Then it is decoding the command.

When 'forward' command is found, MCU triggers another driver IC named LM293D which is a dual motor driver IC. This LM293D has 4 inputs and 4 outputs. 2 enable pins are used to enable the channel. Input 1&2 are associated with output 1&2 and Enable 1 is controlling these two pins. Like this way, En2 controls other 2 i/o s. When motor need to run forward, in1 is high, in2 is low for both motor. On the other hand when motor need to run backward, in1 is low, in2 is high. Like this input left or right turns are made.

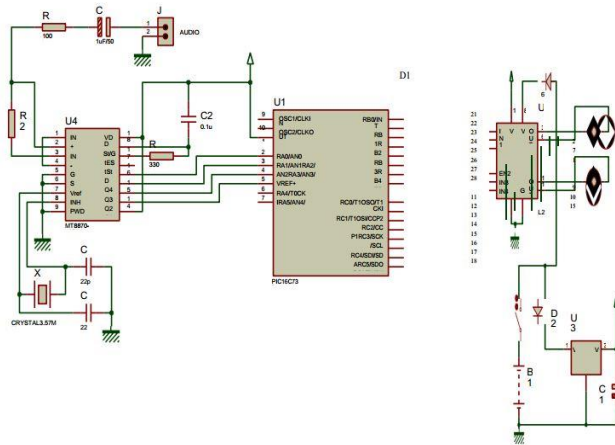


Figure 4: Circuit diagram of our project

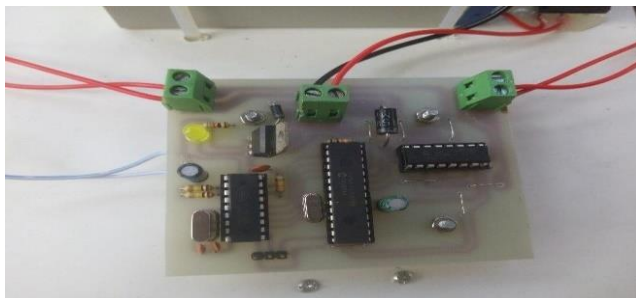


Figure 5: Experimental image of circuit

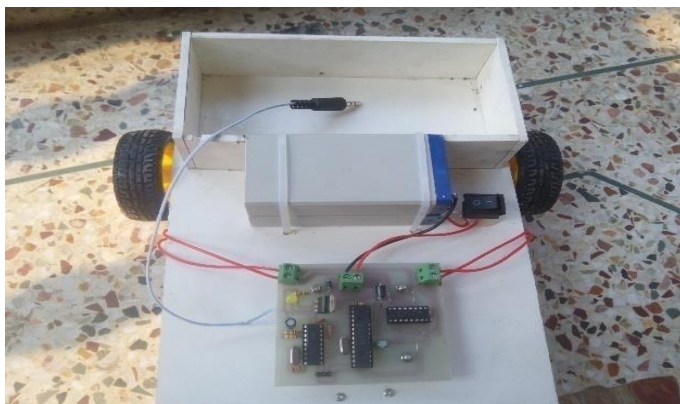


Figure 6: Experimental image of our project

V. COST ANALYSIS

A. Battery volt consumption:

Used 9v battery to our system which can performed about 36 hours. But we monitored our system for an hour. Here is the chart of using amount of voltage of our constructed device during monitoring time:

Time(Hour)	Voltage(Volt)
36	9
27	6.75
18	4.5
9	2.25
1	0.2

Table 1: Voltage Consumption

So, during our experimental time we used 0.2 volt of 9 volt battery.

B. Time of searching:

We calculated the time that needed to our system for searching objects using the law of velocity(v), distance(s), time(t).

$$V = s/t$$

$$\text{So } t = s/v$$

$$V = 3.6 \text{ for our dc motor}$$

We calculated this in different criteria, such as-

No Object: When there was no object in the room our system search the entire room for the object and it took 1.52 minutes to finish..

Object in free space: When there was no barrier we kept our object in distance of 300sq.ft and our system took 0.415 minutes to find the object.

Object hidden behind barrier: For last we kept an object in distance about 400 sq.ft and we hid our system behind barriers that made the distance about 700 sq.ft from the object. Finally our device took 0.96 minutes to search for it.

Calculation:

$$t = s/v$$

$$v = 3.67 \text{ m/s for our dc motor}$$

$$1 \text{ sq.ft} = 0.3048 \text{ m}$$

Criteria	Distance(sq.ft)	Velocity(m/s)	Time(minute)
No object	1100	3.76	1.52
Object in free space	300	3.76	0.415
Object hidden behind barrier	700	3.76	0.96

Table 2: calculation of searching time

VI. CONCLUSION AND FUTURE SCOPE

Constructed and figured the 'MOBILE CONTROLLING ROBOT' in enough less cost which might help in various steps and we can assure that it will handle different situations in very smart way. This type of wireless communication will cause many advantages such as robust control, minimal interference and a large working range. We can also control it with the app "DTMF tone generator. Till now MOBILE CONTROLLING ROBOT concept is used widely. This

project was implemented by many others before but ours is best as We tried to build it at very cheaper cost and we desire to work with it for further options.

WORKS CITED

- [1] India, P. (2017). A Chinese restaurant where robots cook and serve food. [online] Businessstandard.com. Available at: http://www.business-standard.com/article/pti-stories/a-chineserestaurant-where-robots-cook-and-serve-food-113011400385_1.html [Accessed 13 Aug. 2017]
- [2] Narasimhan, T. (2017). Ford installs 92 robots at Chennai unit. [online] Businessstandard.com. Available at: http://www.business-standard.com/article/companies/ford-installs-92-robots-at-chennai-unit-110071700038_1.html [Accessed 13 Aug. 2017].
- [3] Cyberdyne.jp. (2017). CYBERDYNE. [online] Available at: <https://www.cyberdyne.jp/english/products/cleanrobot.html> [Accessed 13 Aug. 2017].

REFERENCES

- [4] Ctahar.blogspot.com. (2017). 10 Things We Couldn't Do Without Robots. [online] Available at: <http://ctahar.blogspot.com/2016/05/10-things-we-couldnt-do-without-robots.html> [Accessed 13 Aug. 2017].
- [5] Anon, (2017). [online] Available at: <https://pdfs.semanticscholar.org/8373/cb0edc5664e70e2601882bae744c2875d54f.pdf> [Accessed 13 Aug. 2017].
- [6] NASA. (2017). NASA Space Robotics Challenge Prepares Robots for the Journey to Mars. [online] Available at: https://www.nasa.gov/directorates/spacetech/centennial_challenges/feature/space_robotics_challenge.html [Accessed 13 Aug. 2017].
- [7] Recode. (2017). Domino's is going to use sidewalk robots in Germany to deliver pizza. [online] Available at: <https://www.recode.net/2017/3/29/15100748/dominos-deliver-pizzarobots-germany-starship> [Accessed 13 Aug. 2017].
- [8] IEEE Spectrum: Technology, Engineering, and Science News. (2017). Japan Earthquake: Robots Help Search For Survivors. [online] Available at: <http://spectrum.ieee.org/automaton/robotics/industrial-robots/japan-earthquake-robots-helpsearch-for-survivors> [Accessed 13 Aug. 2017].
- [9] Corner, L. (2017). All About 7805 IC | Voltage Regulator Pin Diagram & Schematics. [online] Electronics For You. Available at: <http://electronicsforu.com/electronics-projects/7805-ic-voltage-regulator> [Accessed 13 Aug. 2017].
- [10] Anon, (2017). [online] Available at: <http://ee.sharif.edu/~sakhtar3/books/8051%20Microcontrollers%20And%20Applications%20Based%20Introduction.pdf> [Accessed 13 Aug. 2017].

QoS Based Scheduling Techniques in Cloud Computing: Systematic Review

Monika, Om Prakash Sangwan, *Guru Jambheshwar University of Science & Technology, Hisar, Haryana*
monikard31@hotmail.com, sangwan0863@gmail.com

Abstract-Cloud computing is the fastest emerging technology and a novel buzzword in the field of IT domain that offer distinct services, applications and focuses on providing sustainable, reliable, scalable and virtualized resources to its consumer. The main aim of cloud computing is to enhance the use of distributed resources to achieve higher throughput and resource utilization in large-scale computation problems. Scheduling affects the efficiency of cloud and plays a significant role in cloud computing to create high performance environment. The Quality of Service (QoS) requirements of user application define the scheduling of resources. Numbers of researchers have tried to solve these scheduling problems using different QoS based scheduling techniques. In this paper, a detail analysis of resource scheduling methodology is presented, with different types of scheduling based on soft computing techniques, their comparisons, benefits and results are discussed. Major finding of this paper helps researchers to decide suitable approach for scheduling user's applications considering their QoS requirements.

Keywords: Scheduling; Soft computing; Cloud Computing; Quality of Service; Review

I. INTRODUCTION

With the significant growth in technology, computing has converted to a commoditized group of services and conveyed in a similar approach to traditional utilities. As a result, users access services according to their requirements without considering basic details of services i.e. where the services are hosted or how they are delivered [1]. Cloud is a dynamic service provider by the use of very large, scalable and virtualized resources pool over the internet. Cloud computing data centers allocates resources to users as per their requirements. During the allocation of resources, following situations may occur: 1) Virtual machine is overloaded and causes low performance (2) virtual machine is under loaded and causes resource underutilization (3) Different applications requires different types of resources [23]. Thus, the allocation of resources to find an optimal schedule for set of jobs is NP-Complete problem [2]. A correct scheduling of tasks depends on various factors i.e. fully analysis of applications before execution, analysis functionalities of available resources, and offer various possible scheduling configuration to help users to identify the optimal configuration to execute applications with minimum overhead. But, there is no such scheduling configuration available for all computing systems that can solve this scheduling problem in polynomial times. However, the best way to select the suitable scheduling technique can be determined by considering characteristics of the network environment, tasks, resources etc. that can work in given environment. Therefore, some of the soft computing techniques have been considered to provide near optimal solutions for these NP-Complete problems. In this paper we have discussed soft computing techniques such as Neural Network, Fuzzy Logic, Genetic Algorithms, Support Vector Machine, Bayesian Network and some of the swarm optimization algorithms i.e. Particle Swarm Optimization (PSO), Simulated Annealing (SA), BAT algorithm and Cuckoo Search Algorithm etc., to identify the major quality of service attributes that effect the performance of scheduling algorithm. We have presented the taxonomy and comprehensive review of these techniques to identify important QoS attributes considered during scheduling in cloud computing.

The paper is organized as follow: Section 2 & 3 describe basic understanding, concepts of resource scheduling and QoS requirement in cloud computing. Section 4 presents the review of various soft-computing techniques based scheduling algorithms and table 1 provides the comparisons of these algorithms based on QoS attributes. In sections 5, we have discussed the

advantages and disadvantages of soft computing techniques and the section 6 shows detail definitions of QoS attributes. Section 7 provides the advantages of resource scheduling techniques. Sections 8 discuss about the major findings or research issues and the future work of the paper has been presented in section 9.

2. RESOURCE SCHEDULING

Resource scheduling is a central concept of cloud computing and put a huge effect on overall performance of cloud service [23]. It is used to identify the suitable resources and provide these resources to customers according to their requirements. The most basic version of scheduling as follows: There are given n jobs i.e. J_1, J_2, \dots, J_n of varying processing times, $R = \{r_1, r_2, \dots, r_m\}$ resources with varying processing power, and there is need to find a mapping function $M.F : J \rightarrow R$ which define the resource R_j to which job j_i is assigned where $1 \leq j \leq n, 1 \leq i \leq m$. The main objective of this mapping function is to minimize complexity, overhead and optimize various QoS attributes. The basic building structure of resource scheduling in cloud computing is shown in fig 1. Jobs are submitted to admission control unit which have complete information about resources and decides whether to accept or reject the job for reschedule according to required job resources. After acceptance of user request, jobs are scheduled to different virtual machine. This first level of scheduling mainly considers QoS demand of user and schedule them on appropriate virtual machine (VM) and the second level scheduler & migrator migrates virtual machines on different physical machines to avoid over or under utilization of resources. The quality of output depends upon the type of virtual machine allocated to task because VM with less failure rate have greater ratio of successfully executing tasks allocated to them, however, with incurs of more cost [65]. Not all users choose high quality of service to finish their work for various reasons i.e. cost of high quality service. So, providers have different varieties of service quality to satisfy all types of requirements, which is the most important practical issue of scheduling problem [16]. There are many basic schedulers available in cloud computing environment. But these schedulers cannot handle task deadlines in efficient manner, and leads to conflict. Thus, soft computing techniques has been widely used for resource scheduling in cloud computing to handle these conflicts between tasks and has been discussed in section 4 of this paper.

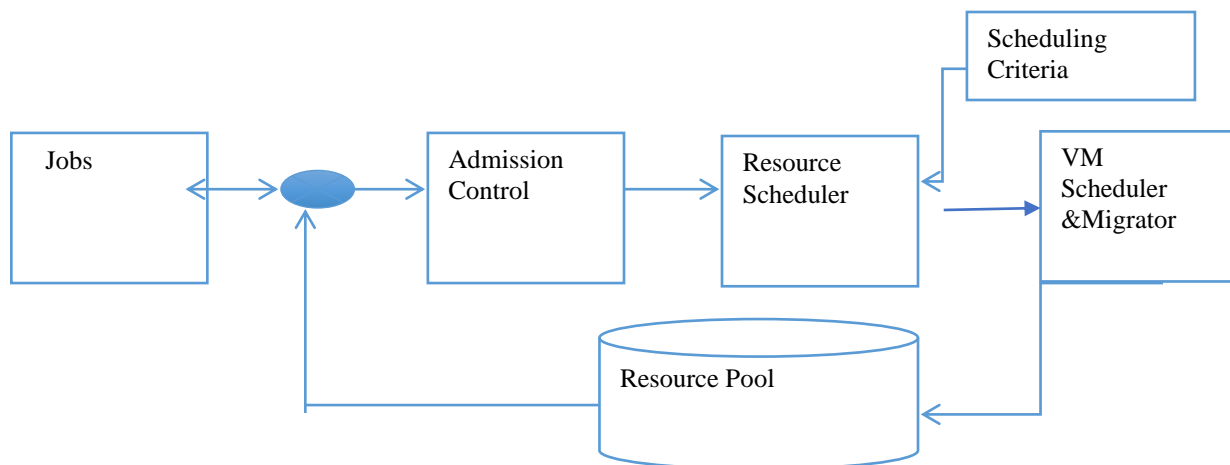


Fig1: Resource Scheduling Flow Chart

III. QUALITY OF SERVICE (QOS)

Quality is a measure of excellence and one of the research issues for cloud system to deliver high QoS to user. It is of great significance to stakeholders, namely service users and providers. Low QoS may result in dissatisfaction and even investment loss

of service users can lead the service providers to pull out of business as it decreases the loyalty of service users. Thus, measurement of quality is an important task to know the quantitative view of quality concept. QoS management is one of the major challenges to deal in cloud applications, having the problem of allocating resources efficiently to applications. Various researchers surveyed various QoS techniques in cloud computing to find out how QoS is related with cloud computing applications and ascertain the extent to which QoS challenged has been resolved in [4-5]. In additional, Amid K. B. and Seyyed M. described [6] various QoS metrics for cloud computing services evaluations. Recent research on QoS approaches in cloud computing, provided by A. Abdelmaboud et al. [7] in order to identify most critical area to be focused in both current and future research work. Every user has its own QoS requirement so, cloud scheduler must be able to schedule the jobs in a way that cloud provider can gain maximum benefit with the QoS satisfaction of user's job [49].

Related Surveys and Mappings

Many researchers have surveyed various issues in cloud computing, and characterize the different problems that affect the efficiency of the cloud services [8-9]. They presented a brief description on the different related approaches applied on current and future scheduling challenges. But, an extensive review of various techniques to support QoS in cloud computing is still missing after substantial research. In this paper, we have done a systematic review of various approaches to cover QoS area in cloud computing.

IV. RESOURCE SCHEDULING USING SOFT COMPUTING TECHNIQUES

Cloud users need their job to be executed with optimal scheduling, less execution time & cost, high reliability and security. Cloud provider priority is to maximize resource utilization, load balancing etc. and to fulfill these priorities, there is a need to find solution that makes proper trade off among all these things [66]. Many soft computing techniques are available for solving such complex problems and in this paper, we have reviewed some of these techniques like, particle Swarm Optimization, Neural Network, Genetic Algorithm etc. These techniques are used to solve various QoS issues related to scheduling of resources in cloud computing environment.

A. Neural Network

ANN is a collection of large number of connected units of artificial neurons working in parallel to solve specific problems [10]. It acquires knowledge through learning and store it within inter neuron connection strength known as synaptic weights. ANN allocates resources according to prediction of demand Therefore, Nada M. et al. [11] used it for achieving load balancing by reducing the resource consumption, energy consumption and further carbon emission rate that is ominous need of cloud computing by using back propagation learning algorithm. F. Almeida et al. [15] used multilayer perceptron with hyperbolic tangent activation function in hidden layer and linear function in output layer to improve scheduling in cloud computing. Comparing with single ANN, the usage of multiple ANN produces better performance, took less time to reduce error and also obtained better response time compared to traditional scheduling algorithms as round robin (22%) and greedy (8%) etc.

Most of the static approaches don't consider VM workload variability during the prediction of resource demand by cloud user, which leads to under, or over provisioning of resources. ANN widely used for forecasting problems, enables it for automate elastic scaling of resources in cloud systems. So, by considering both the dynamic workload fluctuations of VM and prediction accuracy into account, M. Uma et al. [12] used ANN to achieve resource demand

based on resource usage statistics obtained from system static collector and dynamic resource scheduling was applied to consolidate the VM to handle variable workload without SLA violation. To improve resources utilization, Anitha N. and Anirban B. [13] used run time instrumentation with each VM to know its usage status of CPU, memory, bandwidth etc. and supplied this gathered information to feed forward neural network to know whether resource allocation needs to be increased or decreased. Whereas, R. Karthikeyan and P. Chitra [14] combined ANN with grey system for task scheduling that takes 3 significant parameter of task i.e. task length, CPU intensive and memory intensive to reduce execution time and power consumption of VM. A fuzzy neural network PID control based task manager [16] was proposed to get the best value of QoS attributes of the nonlinear and time varying system. The proposed task manger takes the feedback of the last round QoS parameters by using fuzzy max-min inference workload measurement and this feedback is provided as input to neural network. The output layer calculates the workload degree by center of gravity defuzzification.

B. Fuzzy Logic

To understand imprecise requirements of specific problems such as scheduling of resources or virtual machines, a fuzzy model must be constructed. Many authors [17-24] have developed different fuzzy models i.e. rules based system to solve scheduling problem and to understand user's fuzzy demand. In order to optimize the performance and load balancing within the cloud, A. Ragmani et al. [17] used concept of global performance indicator (GPI) based on fuzzy logic theory to rank the difference between possible configuration of physical and virtual machines. To find the best value of GPI, authors considered the variations in input parameters i.e. number of virtual machines and host per datacenters, processor speed, process number, user request and data size etc. A dynamic scheduling algorithm by utilizing fuzzy logic controller is proposed by Amin M. and Seyyed M. H. [18] that fairly assign virtual machines to host by investigating the effect of waiting time slot in the queue and their precedence to reduce the completion time of jobs, as a result, produce an accurate scheduling. M. Zavvar et al. [19] utilized fuzzy metrics of cost, trust and length to provide accurate resource scheduling algorithm based on fuzzy logic to enhance the reliability of cloud computing. To minimize the task waiting time of the precedence-constrained applications [20-22] used fuzzy clustering algorithms. F. Guo et al. [20] considered the resource characteristics i.e. processing and Communication capacity, network location, number of links etc. of processing units of cloud computing and fuzzy similar matrix to form clustering, while Jian Li et al. [21] used radial basis function based fuzzy c- means clustering method to narrow the range of resources by dividing them in three categories: Compute, Storage and Transmission resources and assign these resources based on the inverse trig function to task by taking the task's expectation using improved FIFO scheduling model . So, identifying the performance of the resources is necessary to choose the processing unit with good comprehensive performance for scheduling of task.

M. S. Shinde and A. k. Kadam [22] used linear programming as an optimization technique along with fuzzy C-Means clustering technique to reduce the overall cost within user specified time and outperform FCFS scheduling algorithm. In most of the above research, the basic QoS standards such as cost, time etc. were considered, but some extended QoS standard such as system friendliness and user experience were not considered. These extended QoS standard enable system to understand system fuzzy requirements. Therefore, Z. Chen et. al. [23] emphasis on system friendliness as their main objective and based on user's long term and continuous resource requirements, a second

moving average method was used for prediction and then a fuzzy control theory was adopted to schedule VM dynamically using friendly mapping between resource prediction model output and available resources.

C. Genetic Algorithm (GA)

Genetic algorithm provides a way of scheduling based on biological concept of population generation where initial population is the set of chromosomes or individuals that are used to represent the space of solutions and every individual in this set is called solution. The individuals which are used to generate a new population are selected according to their fitness values i.e. these individuals follow Darwinian theory [25] of “survival to the fittest”. This process is repeated until a best solution that satisfies minimum criteria is produced. The size of initial population varies according to the nature of the problem and it can be represented in different ways i.e. binary [28,32], floating point encoding, Integer [31] and permutation representation. Different researchers generated the set of initial population randomly [26,28,32] and O. Morariu et al. [26] applied this random population GA in private cloud for workload scheduling by considering the effect of primary factors on performance in a virtualized environment. P. kumar and A. Verma [27] make use of Min-Min and Max-Min algorithms to generate initial population and do not only produce better initial population than randomly generated initial population but also reduce makespan by make use of maximum amount of resources. Individual similarity is used by J. Li and C. Qu [31] to ensure the uniformity of initial population in solution space.

After generation of initial generation, the fitness value of each individual is calculated according to fitness or objective function i.e. makespan [27,30-32], Cost [28-31], deadline [29] etc. are used as commonly fitness objective. In some cases, fitness function or objective function may be same, while in others it may be different dependent upon the problems. From the initial population some of the fittest individuals are selected, who will contribute their genes to their children in next generation. Selection operator helps in to improve the convergence speed of algorithm so, different methods has been explored by different researchers to optimize selection procedure i.e. roulette selection [28,30,31], collaborator selection [29], tournament selection [32], rank selection, best 65 % individuals [26] etc. After selection of individuals, crossover and mutation operations are performed on these individuals to generate some new child chromosomes. Most commonly used crossover operators are: single point [27], multipoint crossover, clustered crossover [30] etc. Y. Wang et al. [28] designed crossover by considering the relevance of individuals and helps in shorten the overall execution time of scheduling. S. Hamad and F. Omara [32] used different crossover operator, in which, two chromosomes were selected for crossover process to generate two new offspring were also considered as offspring. So, this proposed operator has four children and after that two best children are chosen from these children. Mutation takes the vales of some gene in chromosome and replaced it by other gene value to generate a new individual. Mutation operator helps in increases diversity of the main population, ability of local search and avoid local premature phenomenon. Different mutation operators like basic bit mutation operator [28,30], a non-uniform operator [31], swap mutation etc. are used in literature. With the new gene values added by mutation, the GA may be able to produce a better generation than the previous one.

D. Bayesian Network

Bayesian network are a type of probabilistic graphical model that represent a set of parameters and their conditional dependencies via a directed acyclic graph. It uses laws of probability for anomaly detection, decision-

making and time series prediction [34]. Naïve Bayesian method used by Fatemeh E. and Sayed M. B. [35] with the aims of creating load balancing scheduling by classification and selection of virtual machines. The selection of highest runtime request helps in increasing the efficiency and utilization of resources. L. Ferdouse et al. [36] proposed Bayesian network based workload scheduling, which used both task and user level scheduling, and utilize posterior probability based scheduling weights among paths by considering dependency among tasks. A dynamic scheduling algorithm was proposed by W. wang and G. zeng for evaluation of the trustworthiness of nodes using Bayesian method [37]. For the selection problem of physical hosts for deploying requested tasks and long-term load balancing effects J. Zhao et al. [38] used Bayesian network with clustering. They used probability theorem and clustering idea to pick the optimal hosts that have most remaining computing power. Deployment and scheduling mechanism of various cloud services in SaaS using stochastic models by considering different QoS attributes i.e. response time, elasticity, working efficiency of unit resources etc. is described in [39].

E. Meta-Heuristics Techniques

Meta-heuristics are of higher-level and modern phenomenon in approximate search to solve complex optimization problems faced in areas like industries, engineering design, business, economics etc. Meta-Heuristic is not problem centric however, it is designed to create or search a suitable algorithm that may find near-optimal solution by using randomization to an optimization problem, especially with limited computation capacity [46]. We have discussed some of the Meta-Heuristics techniques used for scheduling in cloud computing, which are as follows:

1. PSO

The PSO technique handles issue by using a population of particles where these particles move around in search space by adopting a simple formula for particle velocity and position [40]. Arrival of user's request, the type and numbers of required VM instances are uncertain in cloud computing. So it may be possible that service provider doesn't able to achieve the required needs while guaranteeing user's QoS during peak demand. To handle this issue, G. Zang and X. Zuo [41] applied standard PSO to get an optimal solution to determine the priorities of tasks by sorting the dimensions of a particle in descending order. A Discrete PSO (DPSO) [42] based task-scheduling algorithm has used binary encoding to represent velocity and position of particle. The smallest position value (SPV) for position updating used by basic PSO performs poor when high variance exists between length of task and computational speed of resources. To solve the bi-objective task-scheduling problem and to remove this SPV problem, S.A Beegom and M.S. Rajasree proposed a new method of generating discrete permutation i.e. integer PSO [43] that used weighted sum approach to achieve pareto optimality, which convert a multi objective optimization problem into single objective one with weights representing preferences among objectives by decision maker and outperform SPV based PSO. F. Ramezani et al. [44] proposed a comprehensive multi objective model by considering the criteria of QoS including minimize execution time by keeping the cost low. The outcome of proposed method provides good trade-off solutions for multi-objective task scheduling problem and helps to maintain QoS optimization objective. Over the years, lots of research work has been done in resource scheduling to get efficient and prominent results in cloud computing. Majority of scheduling algorithms consider only cost, time, makespan, resource utilization etc. as their objective and compromise over other QoS attributes i.e. scalability, reliability, availability, throughput etc. because of complexity to achieve these parameters. So A.I. Awad et al. [45]

proposed a mathematical model for load balancing using PSO based scheduling algorithm that takes into account reliability, execution time, transmission time, availability and load balancing between tasks and virtual machines. It achieves the reliability by considering the available resource and reschedule task that fails to allocate by considering the account load of each VM. An ACO with PSO (ACOPS) method proposed by K.M. Cho et al. [46] to solve load balancing problem by scheduling randomly generated request using historical data to predict the demand of new I/P requests. To achieve results of high quality, proposed model used procedure of pre-reject to accelerate computing time and reduce solutions' dimensions, search operator to new paths for all ants, PSO operator to improve search results and used global pheromone update operator that increase pheromone only on current best solutions.

2. *Simulated Annealing (SA)*

The SA is a probabilistic technique used for global optimization in large search space. The cooling process of SA makes it effective to find optimal solution when dealing with large search space that have numerous local optima. At each iteration of SA algorithm, the objective function value for two solutions are compared & based on probability distribution of objective, the algorithm accepts the solution that lower the objective, while some of non-improving solutions are also accepted to escape algorithm from local optima in search of global optima [47,48].

An experiment with random initial solution [50,53,54] takes long calculation time before proceeding for optimal solution. Therefore, GA-Hint approach using opposite () function [49], SQF (shortest queue first) [51], greedy strategy using longest task priority principle [52] etc. used by different researchers to obtain the good initial solution for SA in job scheduling. To ensure QoS requirement of user job, M. Abdullah [49] used inversion move to calculate random solution and their associated cost. I.A. Moschakis and H.D. Karatza [51] evaluated the use of thermodynamic SA (TSA) in the scheduling of bag of task application with virtual machine of heterogeneous performance, where search space is consisting of different permutations of the schedule. In TSA, the cooling schedule is not static and it determined by entropy and energy difference created by state transition using the first and second laws of thermodynamics. E. Torabzadeh and M. Zandieh implemented the basic concept of cloud theory with simulated annealing (CSA) [50] to solve the scheduling problem in two stage assembly flowshop with decrement in the probability of local optima because Cloud theory escape algorithm from being stuck in local optima by preserving diversity (having stable tendency) and relating quality concepts with quality data in comparison to SA that uses hill climbing moves for local search escape from local minimum. Researchers used many different methods in combination of basic SA i.e. Boltzman probability accept function [52], Etropolis criteria [53,55], Powell algorithm [54] to achieve the fast convergence of optimal solutions and to lower possibility of miss the optimal solutions.

3. *Cuckoo Search Algorithm (CSA)*

X. S. Yang and S. Deb proposed Cuckoo optimization algorithm in 2009 after in-depth study of parasitism of some cuckoo species that lay their eggs in nests of host birds. As cuckoos are proficient in the mimicry in pattern and colors of chosen host species eggs, it lessens the probability of eggs being abandoned and increases the probability of their reproductivity. The basic CSA has been applied in scheduling of resources by the consideration of different searching i.e. robust search [59], random search which follow a proper-law step-length distribution with a heavy tail [57,58] and next population generation mechanism i.e. levy flight [57-59] to achieve the different QoS

requirements of users. In the addition of above CSA algorithm, some other constraints were also considered for allocation of task to resources like the length of execution of tasks [57,59], processing power of VM [59] etc. The result of CSA in scheduling shows that the speed and coverage of CSA start increasing with low value of Pa.

Various other techniques have been combined with cuckoo search by researchers to further optimize some other QoS attributes. A combination of GA and CSA used by S. Aujla and A. Ummat [60] in which first GA is used to schedule and this order of scheduling is used by CSA based scheduler to reschedule by checking information of available resources to reduce the failure ratio. To generate the best order of available resources as their initial population, all of the possible order of resources with their objective values considered by A. Moradbeiky and V. bardsiri [61] and obtained results from each order are grouped into 2 clusters by use of k-means clustering. Cluster with better orders were selected for next generation and for each outcome, new result is generated within egg laying radius using levy distribution. To handle the scheduling of tasks on heterogeneous system, M. Akbari and H. Rashidi [62] proposed a multi-objective scheduling method that use the concept of cuckoo algorithms i.e. laying and immigration. This method initially takes random schedules and in generation of new schedule, a processor and task in modifications radius limits the replacement of random processor and task. Later in immigrating stage, all schedules were immigrated towards global optimum point that helped in search of a more expanded area with no involvement in local optima.

4. *BAT Algorithm (BA)*

Echolocation behavior of micro bats inspired Xin-she Yang to develop The BAT algorithm (BA) in 2010. Bats release sonar signals to avoid close obstacles in dark and to detect its prey by transforming sound pulses into frequency [63,64]. This basic bat algorithm is applied by different researchers to solve the multi-objective problems of workflow scheduling with the objective of maximizing reliability and minimizing execution time and it also ruled out the schedules of cost exceeds to budget constraints [65-66]. Though the basic Bat algorithm is mainly used for continuous optimization, S. Raghavan et al. [67] added some aspects of binary algorithm along with bat algorithm to handle discrete set of inputs for scheduling workflow applications in cloud. However, the update process of velocity in the binary BAT is still consistent with BA, therefore, it is not good enough for exploration and exploitation, and may get stuck to local minima. Therefore, in order to overcome this issue, X. Huang et al. [69] proposed improved binary BAT algorithm that uses neighbor bat and dynamic inertia weight strategy to carry out a more diversified search process to avoid being trapped into local minima. Generally, standard BAT algorithm exploits search space by random walks and its fast convergence is not guaranteed because of its tendency to trap in local optima. Therefore, other techniques had been combined with basic BAT algorithm to escape from local optima i.e. chaotic [68] map is used to tune BAT basic parameter using sinusoidal map to initialize pulse emission rate and iterative map for loudness frequency initialization, harmony search is also used by S. Kumar and Aramudhan [70] with BAT by applying trust model to reduce failure ratio and harmony search i.e. a music based meta-heuristics optimization algorithm helps to find optimality in optimization.

Here, we have discussed more than 70 research papers of resource scheduling using soft computing techniques to identify both advantages and disadvantages of every technique used.

V. PROS AND CONS OF SOFT COMPUTING TECHNIQUES

ANN is used for complex problems, pattern classification and recognition. It learns to classify new inputs that have not seen in search space before, while GA finds best solutions within search space. ANN performs better than traditional scheduling algorithms as round robin and greedy in terms of response time and throughput [13,15]. Fuzzy Logic function is to handle impreciseness and uncertainties in the system and the simulation results showed the effectiveness of Fuzzy logic as compared to FCFS and Round Robin, Min-Min and Max-Min in terms of completion time, waiting time etc [18,19]. GA is a meta-heuristic based on genetic evolution with the feature of combinational optimization. GA [29] showed that Cooperative coevolutionary GA always found better solution and scale up well when problem size increases as compared to random GA.

SA major advantage over other methods is its ability to prevent being stuck in local minima and it is mostly known for its effectiveness in finding near optimal solutions for large-scale combinatorial optimization problems. SA converges faster than GA and outperforms GA by a larger gap when running time is considered. SA has better performance when the numbers of jobs are less, while the number machines and jobs are more than 100, GA performs better than SA [49]. The main drawback of SA is its time consuming trait. BAT has automatic zooming capacity & use parameter control to automatically switch from exploration to exploitation when optimal solution is approaching. But it converges very quickly at early stage & then convergence rate slows down & may lead to stagnation after some initial stage [66]. Ease of implementation and fast convergence is the advantages of PSO over many other optimization algorithms [42]. During scheduling task, PSO outperform GA and Min-Min in terms of deadline missing ratio, makespan, cost and load balancing [42]. PSO performance better than GA in every other aspect. The experiment results show that PSO algorithms not only converge faster but also run faster than GA [45]. Cuckoo search and SA consume larger time and cost compared to firefly algorithms [14].

VI. QOS ATTRIBUTES

To identify the important QoS attributes in resource scheduling, we have performed a details analysis of various scheduling techniques as shown in table 1. We have classified these QoS of various scheduling algorithm into two perspectives: service user and service provider. Cloud service providers are the companies which offer some services like network; infrastructures etc. to other businesses or individuals and cloud service users, use these services to accomplish their tasks by using pay-as-you-use or pricing models. The classification of scheduling QoS attributes is presented in fig 2.

A. *Service User Objective Attributes*

These are some of the essential QoS attributes that a user requires to run its application in an efficient manner.

1. *Makespan*

It is the total time required by a group of jobs to finish its execution from beginning to end. A good scheduler always tries to reduce makespan as much as possible. It is one of the methods to measure efficiency.

2. *Cost*

The cost of the job execution depends upon the cost of many other services i.e. computation, storage & transmission etc. A good scheduler always tries to minimize this cost.

3. *Scalability*

It is one of the key benefit and ability of cloud computing to continue to work, when there is change in the size of user demand or its potential to be enlarged in order to accommodate that growth. Scalability is more granular than elasticity when it comes to sizing.

4. *Dead Line*

It defines the latest time, day or date, before some tasks must be completed.

5. *Reliability*

It is the ability of computer hardware and software to consistently work according to the requirements. Reliability is necessary to ensure the stability of the system and it also affects the usability of services.

6. *Efficiency*

Cloud computing is a new approach for making efficient use of computing resources and it is improved by combining various cloud applications per virtual machine or physical hosted servers.

B. *Service Provider Objective Attributes*

The following are the QoS attributes that a service provider needs to manage to satisfy the requirement of service users and to make profit.

1. *Load Balancing*

It is key aspect of cloud computing and the process of distributed workloads, computing resources across one or more servers so that no node become overloaded while other is idle at the same time. It has impact on other QoS metrics, such as: response time, cost, throughput, load balancing etc. [71].

2. *Resource Utilization*

Utilization of resources affects the overall efficiency of cloud. Resource utilization differs for each task based on task requirement and it increases if the task takes up and makes use of only required resources [14].

3. *Throughput*

It is a measure of average amount of data that can be transferred per unit of time and provide the performance of a processor, memory or a network.

4. *Energy*

Cloud is energy efficient because of economies of scale, diversity and aggregation. It is not only determined by hardware efficiency but also affected by other factors i.e. resource management system, efficiency of system etc.

5. *Fault Tolerant*

It is the ability of infrastructure to continue providing services even after the failure of some of its components. The system will not run with full of its efficiency but it will run at a reasonable level.

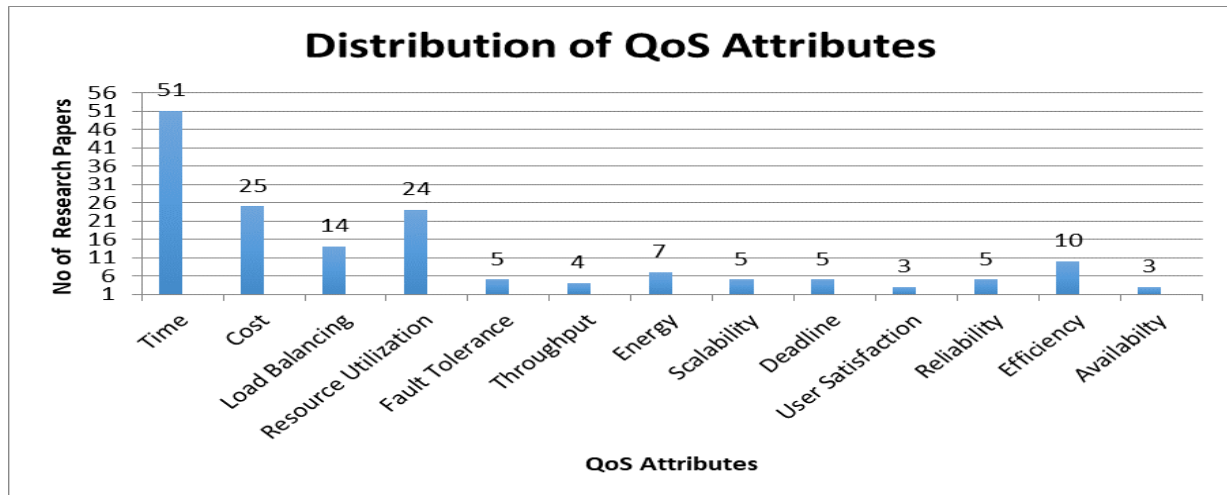


Fig 2: Distribution of QoS Attributes

6. Availability

High Availability is the ultimate goal of cloud computing. Availability allows users to access services according “pay as you go” policy without concern about location. It refers to the ability of user to access information, services and tools anywhere and anytime.

VII. ADVANTAGES OF RESOURCE SCHEDULING

We have identified number of advantages of resource scheduling from above literature, some of the important are:

1. Use of underutilized server by multiple VM increases the resource utilization rate [11].
2. The efficient strategy handles criteria's i.e. less resource shuttering and conflicting, over provisioning and under provisioning etc.
3. Performance of VM helps scheduler to assign new tasks to suitable machines.
4. Average success rate improve the efficiency of scheduling between conflict resource demands [24].
5. Virtualization helps to improve resource availability, reduce complexity and avoids infrastructure-associated risks.
7. Its scalability, flexibility helps users to handle dynamic requirements of users.
8. Efficient cloud resource allocation and scheduling reduces waiting time of tasks in workload queue.
9. Minimum chances of scheduling delay and resource failure due to efficient allocation of resources.
10. Efficient scheduling reduces energy consumption without violation of SLA.
11. Scheduling decisions finished in shortest time is useful for competence between resource and time [16].

VIII. CHALLENGES IN RESOURCE SCHEDULING

We also come across various problems and challenges still faced by researcher in resource scheduling environment and these challenges are briefly described in table 2. This survey can help user to identify current trends and techniques used in cloud environment effortlessly.

TABLE 2: CHALLENGE/OPEN ISSUES IN EXISTING RESOURCE SCHEDULING TECHNIQUES

Techniques	References	Description	Challenge/Open Issues
Neural Network	[11]	Proposed a framework for equally distribution of workload using back propagation learning algorithm to train forward ANN to handle energy consumption.	Extensive use and growing demand of cloud network harshly increasing the energy consumption of data centers thus increasing cost and carbon emission.
	[12]	Proposed a neural based prediction strategy to handle elastic resource scaling by considering dynamic workload fluctuations and prediction.	How to handle resources on the virtual machines for management of variable load without SLA violation?
	[13]	Discussed a dynamic resource allocation using application current status, transactions per second and parameters for resource usage to decide the number of resource needed.	It is difficult for this process to describe that in which order the processes must run to get a proper benchmark of utilization of resources.
	[14]	Developed a framework by considering some significant factors such as task length, CPU and memory intensive to reduce the execution time and energy consumption.	How to handle the time delay caused by switching off and on of resources with efficient energy consumption for fluctuating demand of resources?
Fuzzy Logic	[17]	To find the suitable matching of VM and servers, it used fuzzy logic to calculate global performance indicators using KPI, i.e. response time, processing time and cost.	How to use this approach to assess the KPI in multi criteria decision problems?
	[20]	A framework with 3 phases: i) resource clustering phase ii) task prioritizing phase iii) processor allocation phase to minimize the schedule length.	Addition of an effective security mechanism in scheduling of workflow task.
	[21]	It used fuzzy c-means clustering to reduce the requirement of resources and execution time of the tasks.	What can be the effects if resource homogeneity further increased?
Genetic Algorithm	[29]	Proposed an scalable algorithm using cooperative coevolution GA for deadline-constrained problem.	What can be the alternative collaborator selection and credit assignment methods to improve the performance?
	[30]	Presented a genetic based approach that provides users with various scheduling configuration and helps user to select optimal configuration.	Effects of fluctuations in the hiring cost of virtual machines.
	[27]	Proposed improved GA based framework by considering makespan as fitness criteria.	Scheduling of tasks as multi criteria decision problem.
PSO	[42]	Used PSO to optimize the objectives including cost, makespan, deadline missing ratio, load balance and maximize the profit of cloud.	How to improve the reliability in the cloud system?
	[44]	Implemented a multi objective PSO to find a good tradeoff between scheduling time and cost.	Effects by considering task priorities, types and dependencies in this scheduling approach.
	[45]	Presented a load balancing PSO to increase the reliability by reschedule the failure tasks to available machines by considering load of each VM.	How to extend it to handle the failure to schedule of jobs to virtual machines?
	[46]	Used PSO + ACO for VM scheduling that uses log information to predict the workload of new coming requests without additional information.	How to upgrade it to further decrease the rate of rejection during increasing size of data set?
Simulated Annealing	[49]	Developed a SA based approach that concerns about execution cost, deadline, penalty cost in different systems.	Evaluation of the algorithm with other QoS parameters.
	[50]	Used cloud based theory simulated annealing process to minimize weighted sum of makespan, mean completion time as their objectives.	Execute this process with some other objectives i.e. makespan, lateness, deadline, profit etc.
	[51]	Proposed a thermodynamics SA based framework that optimize cost and performance into heterogeneous environment.	How to achieve inter cloud level seeking for fair spread of parallel between clouds.
Cuckoo Search	[58]	Describe use of cuckoo search to minimize total time and cost of execution.	What is the best way to rank the tasks of a workflow?
	[62]	Described a multi objective algorithm based on cuckoo optimization algorithm to optimize execution time, cost etc.	Best way to generate initial population in cuckoo search and other meta heuristics algorithm.
BAT algorithm	[68]	Proposed a framework based on BAT with the help of chaos theory to optimize the makespan and energy consumption.	How chaotic maps help to improve the performance of the scheduling algorithm?

TABLE 1: QOS ATTRIBUTES IN DIFFERENT RESOURCE SCHEDULING TECHNIQUES

Reference	QoS Attributes												
	Time	Cost	Load Balancing	Resource Utilization	Fault Tolerance	Throughput	Energy	Scalability	Dead line	User Satisfaction	Reliability	Efficiency	Availability
[11]	√	-	-	√	√	√	√	√	-	-	-	-	-
[12]	-	-	-	√	-	-	-	-	-	-	-	-	-
[13]	√	-	-	√	-	-	-	-	-	-	-	-	-
[14]	√	-	-	√	-	-	√	-	-	-	-	-	-
[15]	√	-	-	√	-	√	-	-	-	-	-	-	-
[16]	√	√	√	√	-	-	-	-	-	√	-	-	-
[17]	√	√	√	-	√	-	-	-	-	-	-	-	-
[18]	√	-	-	-	-	-	-	-	-	-	-	-	-
[19]	√	√	-	-	-	-	-	-	-	-	√	-	-
[20]	√	-	-	-	-	-	-	-	-	-	-	√	-
[21]	√	-	-	√	-	-	-	-	-	-	-	-	-
[22]	√	√	-	-	-	-	-	-	-	-	-	-	-
[23]	√	√	-	√	-	-	-	-	-	-	-	√	√
[24]	√	-	-	√	-	-						√	√
[26]	√	-	-	-	-	-	-	-	-	-	-	-	-
[27]	√	-	-	√	-	-	-	-	-	-	-	-	-
[28]	√	√	-	-	-	-	√	-	-	-	-	-	-
[29]	√	√	-	-	-	-	-	√	√	-	-	√	-
[30]	√	√	-	√	-	-	-	-	-	-	-	-	-
[31]	√	√	-	-	-	-	-	-	-	-	-	-	-
[32]	√	√	-	√	-	√	-	-	-	-	-	√	-
[33]	√	√	-	√	-	-	√	-	-	-	-	-	-
[35]	√	-	√	√	-	-	-	-	-	-	-	√	-
[36]	√	-	-	-	-	-	-	-	-	-	-	-	-
[37]	√	-	-	-	√	-	-	-	-	-	√	-	-
[38]	√	-	√	-	-	√	-	-	-	-	-	-	-
[39]	√	-	√	√	-	-	-	√	-	-	-	√	-

Reference	Time	Cost	Load Balancing	Resource Utilization	Fault Tolerance	Throughput	Energy	Scalability	Dead Line	User Satisfaction	Reliability	Efficiency	Availability
[41]	√	√	-	-	-	-	-	-	√	-	-	-	-
[42]	√	√	√	√	-	-	-	-	√	-	-	-	-
[43]	√	√	-	-	-	-	-	-	-	√	-	-	-
[44]	√	√	-	-	-	-	-	-	-	-	-	-	-
[45]	√	√	√	-	-	-	-	-	-	-	√	-	√
[46]	√	√	√	√	-	-	-	-	-	-	-	-	-
[49]	√	√	-	-	-	-	-	-	√	-	-	-	-
[50]	√	-	-	-	-	-	-	-	-	-	-	-	-
[51]	√	√	-	√	-	-	-	-	-	-	-	-	-
[52]	√	-	-	√	-	-	-	-	-	-	-	-	-
[53]	√	√	√	-	-	-	-	-	-	-	-	√	-
[54]	√	-	√	-	-	-	-	-	-	-	√	√	-
[55]	-	-	√	√	-	-	√	√	-	-	-	-	-
[73]	√	√	√	-	-	-	-	-	-	-	-	-	-
[57]	√	-	-	-	-	-	-	-	-	-	-	-	-
[58]	√	√	-	√	-	-	-	-	√	-	-	-	-
[59]	√	-	-	-	-	-	-	-	-	-	-	-	-
[60]	√	-	-	√	√	-	√	-	-	-	-	-	-
[61]	√	-	√	-	-	-	-	-	-	√	-	-	-
[62]	√	√	-	-	-	-	-	-	-	-	-	-	-
[65]	√	√	-	-	-	-	-	-	-	-	√	-	-
[66]	√	-	√	√	-	-	-	√	-	-	-	-	-
[67]	√	√	-	-	-	-	-	-	-	-	-	√	-
[68]	√	-	-	-	-	-	√	-	-	-	-	-	-
[69]	√	-	-	√	√	-	-	-	-	-	-	-	-
[72]	√	-	-	-	-	-	-	-	-	-	-	-	-

IX. CONCLUSION AND FUTURE SCOPE

Resource scheduling has been widely used in cloud computing in order to improve the efficiency of resource utilization and to increase task performance. Various kind of scheduling algorithms have been used by various researchers, were discussed systematically in this paper. It was found that soft computing techniques namely Neural Network, Fuzzy Logic, Genetic Algorithm, Bayesian Network and meta heuristics techniques are widely used by researchers for resource scheduling based on different QoS attributes. In this paper, we have done comparison of existing algorithms based on major QoS parameters like Time, Cost, Resource Utilization, Efficiency, Energy etc. Advantages and challenges of existing resource scheduling techniques were also discussed in this paper and found that there is no single technique exists that provide a better scheduling in cloud environment. It is concluded that the performance of cloud computing environment is not only dependent on resource scheduling techniques but also depend upon QoS attributes.

A. Future Scope

1. Need to develop energy efficient solutions to address high-energy consumption problem from the viewpoint of environment and cloud provider [21].
2. Scaling techniques are required to determine the required number of servers [22].
3. Develop a resource allocation mechanism to handle resource allocation in collaborative cloud computing [23].
4. How to increase the friendliness of system to handle imprecise demand of user [35]?
5. Find a practical schedule to meet the constraints of multi-objectives scheduling problems is a challenging task [59].
6. Applying proposed algorithms in real cloud computing environment [62].
7. In spite of exponential growth of cloud computing there remain several gaps in the growth of cloud model [1].
8. Time and cost are conflicting parameters that need to be balanced and optimized [21].
9. In case of multi-objective problem, we can't get single best solution, so we have pareto set of solution representing trade-off front among multiple considered objectives [24].
10. QoS based resource scheduling is still an issue.

We hope that this research work will be beneficial for researchers who want to work in the field of scheduling in cloud computing environment.

REFERENCES

- [1] R. Buyya and S. Vazhkudai, "Compute Power Market: Towards a Market-Oriented Grid," *ACM International Symposium on Cluster Computing and the Grid*, pp. 574–581, 2001.
- [2] J. D. Ullman, "NP-Complete Scheduling Problems," *Journal of Computer and System Sciences*, vol. 10, no. 3, pp. 384–393, Jun. 1975.
- [3] Kshirasagar Naik, Priyadarshi Tripathy, "Software Testing and Quality Assurance: Theory and Practice," Wiley Publication, pp. 648, 2008.
- [4] H. Akpan, Akpan, B. Rebeccajeya, and Vadhanam, "A Survey on Quality of Service in Cloud Computing," *International Journal of Computer Technology and Trends*, vol. 27, pp. 58–63, Oct. 2015.
- [5] Hashem H. Ramadan, Dr. Divya Kashyap, "Quality of Service (qos) in Cloud Computing", *International Journal of Computer Science and Information Technologies*, Vol. 8 (3), 2017, 318-320.
- [6] Amid Khatibi Bardsiri, Seyyed Mohsen Hashemi, "QoS Metrics for Cloud Computing Services Evaluation", *International Journal of Intelligent Systems and Applications*, 2014, vol 12. Pp 27-33.
- [7] A. Abdelmaboud, D. N. A. Jawawi, I. Ghani, A. Elsafi, and B. Kitchenham, "Quality of Service Approaches in Cloud Computing: A Systematic Mapping Study," *Journal of Systems and Software*, vol. 101, no. Supplement C, pp. 159–179, Mar. 2015.
- [8] P. Singh, M. Dutta, and N. Aggarwal, "A Review of Task Scheduling Based on Meta-heuristics Approach in Cloud Computing," *Knowledge and Information System*, vol. 52, no. 1, pp. 1–51, Jul. 2017.
- [9] S. Singh and I. Chana, "A Survey on Resource Scheduling in Cloud Computing: Issues and Challenges," *Journal of Grid Computing*, vol. 14, no. 2, pp. 217–264, Jun. 2016.
- [10] W. S. McCulloch and W. Pitts, "The Statistical Organization of Nervous Activity," *International Biometric Society*, vol. 4, no. 2, pp. 91–99, 1948.
- [11] Nada M. Al Sallami, Jordan Ali Al daoud, Sarmad A. Al Alous, "Load Balancing with Neural Network", (IJACSA) *International Journal of Advanced Computer Science and Applications*, Vol. 4, No. 10, 2013, pp. 138-145.
- [12] M. Uma, Partha Sarathi Chakraborty, "Neural Network Prediction Based Dynamic Resource Scheduling for Cloud System", *International Journal on Recent and Innovation Trends in Computing and Communication* Vol. 4, Issue 3, pp. 474-477, 2016.
- [13] Anitha N, Anirban Basu, "Neural Network Based Resource Allocation Using Run Time Instrumentation with Virtual Machine Migration in Cloud Computing", *International Journal of Emerging Science and Engineering (IJESE)*, Volume-3 Issue-3, January 2015, pp 27-29.
- [14] R. Karthikeyan, P. Chitra, "Novel Power Reduction Framework for Enhancing Cloud Computing by Integrated Gsnn Scheduling Method", *Cluster Computing*, Vol. 20, Issue 78, 2017, pp 1-12.
- [15] F. F. d Almeida, A. d A. Neto, and M. M. Teixeira, "Resource Scheduling in Web Servers in Cloud Computing using Multiple Artificial Neural Networks," in *2015 Fourteenth Mexican International Conference on Artificial Intelligence (MICAI)*, 2015, pp. 188–193.
- [16] Xiaoqi Xing, Bin Liu and Dongyi Ling, "Neural Network pid Control Based Scheduling Mechanism for Cloud Computing", *Applied Mathematics & Information Sciences*, Vol. 9, Issue 2. 2015, pp. 789-796.
- [17] A. Ragmani, A. El Omri, N. Abghour, K. Moussaid, and M. Rida, "An Improved Scheduling Strategy in Cloud Computing using Fuzzy Logic," in *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*, New York, NY, USA, 2016, p. 22:1–22:9.
- [18] Amin Mehrzadeh, Seyyed Mohsen Hashemi, "A Novel-Scheduling Algorithm for Cloud Computing Based on Fuzzy Logic", *International Journal of Applied Information System*, Vol. 5, Issue 7, 2013, pp 28-31.
- [19] M. Zavvar, M. Rezaei, S. Garavand, and F. Ramezani, "Fuzzy Logic-Based Algorithm Resource Scheduling for Improving the Reliability of Cloud Computing," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 5, no. 1, pp. 39–48, Jun. 2016.
- [20] F. Guo, L. Yu, S. Tian, and J. Yu, "A Workflow Task Scheduling Algorithm Based on the Resources' fuzzy Clustering in Cloud Computing Environment," *International. Journal of Communication System*, vol. 28, no. 6, pp. 1053–1067, Apr. 2015.
- [21] Jian Li, Tinghuai Ma, Meili Tang, Wenhai Shen 3 and Yuanfeng Jin, "Improved FIFO Scheduling Algorithm Based on Fuzzy Clustering in Cloud Computing", *Information (MPDI)*, Vol. 8, issue 1, 2017. doi:10.3390/info8010025.
- [22] Mahesh S. Shinde1, Anil kumar Kadam, "Cloud Based Task Scheduling using Fuzzy C-Means and Linear Programming Approach", *International Journal of Science and Research (IJSR)*, Vol. 4, Issue 7, july 2015, PP 2081-2085.
- [23] Zhijia Chen, Yuanchang Zhu, Yanqiang Di, and Shaochong Feng, "A Dynamic Resource Scheduling Method Based on Fuzzy Control Theory in Cloud Environment," *Journal of Control Science and Engineering*, vol. 2015, Article ID 383209, 10 pages, 2015. doi:10.1155/2015/383209
- [24] P. V and C. Nelson Kennedy Babu, "Moving Average Fuzzy Resource Scheduling for Virtualized Cloud Data Services," *Computer Standards & Interfaces*, vol. 50, no. Supplement C, pp. 251–257, Feb. 2017.
- [25] D. B. Paul, "The Selection of the 'Survival of the Fittest,'" *Journal of the History of Biology*, vol. 21, no. 3, pp. 411–424, 1988.
- [26] O. Morariu, C. Morariu, and T. Borangiu, "A Genetic Algorithm for Workload Scheduling in Cloud Based E-Learning," *2Nd International Workshop on Cloud Computing Platforms*, New York, NY, USA, 2012, p. 5:1–5:6.
- [27] P. Kumar and A. Verma, "Scheduling Using Improved Genetic Algorithm in Cloud Computing for Independent Tasks," *International Conference on Advances in Computing, Communications and Informatics*, New York, NY, USA, 2012, pp. 137–142.
- [28] Y. Wang, J. Wang, C. Wang, and X. Song, "Resource Scheduling of Cloud with QoS Constraints," in *Advances in Neural Networks – ISNN 2013*, 2013, pp. 351–358.
- [29] L. Ai, M. Tang, and C. Fidge, "Resource Allocation and Scheduling of Multiple Composite Web Services in Cloud Computing Using Cooperative Coevolution Genetic Algorithm," *Lecture Notes in Computer Science*, vol. 7063, pp. 258–267, Nov. 2011.
- [30] I. Casas, J. Taheri, R. Ranjan, L. Wang, and A. Y. Zomaya, "GA-ETI: An Enhanced Genetic Algorithm for the Scheduling of Scientific Workflows in Cloud Environments," *Journal of Computational Science*, Sep. 2016.
- [31] J. W. Li and C.-W. Qu, "Cloud Computing Task Scheduling Based on Cultural Genetic Algorithm," *MATEC Web of Conferences*, vol. 40, pp. 9008-p.2-p.5.
- [32] Safwat A. Hamad, Fatma A. Omara, "Genetic-Based Task Scheduling Algorithm in Cloud Computing Environment", *International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 4, 2016, pp. 550-556.
- [33] M. Mezmaz et al., "A Parallel Bi-Objective Hybrid Metaheuristic for Energy-aware Scheduling for Cloud Computing Systems," *Journal of Parallel and Distributed Computing*, vol. 71, no. 11, pp. 1497–1508, Nov. 2011.
- [34] D. Heckerman, A. Mamdani, and M. P. Wellman, "Real-World Applications of Bayesian Networks," *Communications of the ACM*, vol. 38, no. 3, pp. 24–26, Mar. 1995.
- [35] Fatemeh Ebadifard, Seyed Morteza Babamir, "Dynamic Task Scheduling in Cloud Computing Based on Naïve Bayesian Classifier", pp. 91-95, 2017.

- [36] L. Ferdouse, M. Li, L. Guan, and A. Anpalagan, "Bayesian Workload Scheduling in Multimedia Cloud Networks," in 2016 IEEE 21st International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), 2016, pp. 83–88.
- [37] W. Wang and G. Zeng, "Bayesian Cognitive Model in Scheduling Algorithm for Data Intensive Computing," *Journal of Grid Computing*, vol. 10, no. 1, pp. 173–184, Mar. 2012.
- [38] J. Zhao, K. Yang, X. Wei, Y. Ding, L. Hu, and G. Xu, "A Heuristic Clustering-Based Task Deployment Approach for Load Balancing Using Bayes Theorem in Cloud Environment," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 305–316, Feb. 2016.
- [39] H. Yang, L. Yang, and F. Lv, "Cloud Computing System Scheduling Model Based on Bayesian Network," 5th International Conference on Information Engineering for Mechanics and Materials, pp. 1122–1126, 2015.
- [40] J. Kennedy and R. Eberhart, "Particle Swarm Optimization," *IEEE International Conference on Neural Networks*, vol. 4, pp. 1942–1948, 1995.
- [41] G. Zhang and X. Zuo, "Deadline Constrained Task Scheduling Based on Standard-PSO in a Hybrid Cloud," in *Advances in Swarm Intelligence*, 2013, pp. 200–209.
- [42] H. Chen and W. Guo, "Real-Time Task Scheduling Algorithm for Cloud Computing Based on Particle Swarm Optimization," in *Cloud Computing and Big Data*, 2015, pp. 141–152.
- [43] A. S. A. Beegom and M. S. Rajasree, "A Particle Swarm Optimization Based Pareto Optimal Task Scheduling in Cloud Computing," in *Advances in Swarm Intelligence*, 2014, pp. 79–86.
- [44] F. Ramezani, J. Lu, and F. Hussain, "Task Scheduling Optimization in Cloud Computing Applying Multi-Objective Particle Swarm Optimization," in *Service-Oriented Computing*, 2013, pp. 237–251.
- [45] A. I. Awad, N. A. El-Hefnawy, and H. M. Abdel_kader, "Enhanced Particle Swarm Optimization for Task Scheduling in Cloud Computing Environments," *Procedia Computer Science*, vol. 65, no. Supplement C, pp. 920–929, Jan. 2015.
- [46] K. M. Cho, P. W. Tsai, C.-W. Tsai, and C.-S. Yang, "A Hybrid Meta-Heuristic Algorithm for VM Scheduling with Load Balancing in Cloud Computing," *Neural Comput & Applic*, vol. 26, no. 6, pp. 1297–1309, Aug. 2015.
- [47] Khachatryan, A.; Semenovskaya, S.; Vainshtein, B. (1979). "Statistical-Thermodynamic Approach to Determination of Structure Amplitude Phases". *Sov.Phys. Crystallography*. 24 (5): 519–524.
- [48] A. Khachatryan, S. Semenovskaya, and B. Vainshtein, "The Thermodynamic Approach to the Structure Analysis of Crystals," *Acta Crystallogr*, vol. 37, no. 5, pp. 742–754, Sep. 1981.
- [49] M. Abdullah, M. Othman, M. Abdullah, and M. Othman, "Simulated Annealing Approach to Cost-Based Multi- Quality of Service Job Scheduling in Cloud Computing Environment," *American Journal of Applied Sciences*, vol. 11, no. 6, pp. 872–877, Mar. 2014.
- [50] E. Torabzadeh and M. Zandieh, "Cloud Theory Based Simulated Annealing Approach for Scheduling in the Two Stage Assembly Flowshop," *Advances in Engineering Software*, vol. 41, no. 10, pp. 1238–1243, Oct. 2010.
- [51] I. A. Moschakis and H. D. Karatza, "Multi-Criteria Scheduling of Bag-of-Tasks Applications on Heterogeneous Interlinked Clouds with Simulated Annealing," *Journal of Systems and Software*, vol. 101, no. Supplement C, pp. 1–14, Mar. 2015.
- [52] Xi Liu and Jun Liu, "A task Scheduling Based on Simulated Annealing Algorithm in Cloud Computing", *International Journal of Hybrid Information Technology*, vol. 9, Issue 6, pp. 403–412, 2016
- [53] Chengfeng Jian, Yekun Wang, Meng Tao and Meiyu Zhang, "Time-Constrained Workflow Scheduling in Cloud Environment Using Simulation Annealing Algorithm", *Journal of Engineering Science and Technology Review*, Vol. 6, Issue-5, 2013, pp. 33–37
- [54] X. F. Deng, "A Dynamic Task Scheduling Strategy Based on mvfsa in Cloud Computing Environment," *Applied Mechanics and Materials*, vol. 427–429, pp. 2596–2599, 2013.
- [55] X. Xu, L. Cao, X. Wang, X. Xu, L. Cao, and X. Wang, "Resource Pre-Allocation Algorithms for Low Energy Task Scheduling of Cloud Computing," *Journal of Systems Engineering and Electronics*, vol. 27, no. 2, pp. 457–469, Apr. 2016.
- [56] X. S. Yang and S. Deb, "Cuckoo Search via Levy Flights," *World Congress on Nature Biologically Inspired Computing (NaBIC)*, 2009, pp. 210–214.
- [57] Nima Jafari Navimipour and Farnaz Sharifi Milani, "Task Scheduling in the Cloud Computing Based on the Cuckoo Search Algorithm", *International Journal of Modeling and Optimization*, Vol. 5, No. 1, 2015, pp. 44–47.
- [58] H. Singh and R. Randhawa, "Cuckoo Search Based Workflow Scheduling on Heterogeneous Cloud Resources," in 2017 7th International Conference on Cloud Computing, Data Science Engineering - Confluence, 2017, pp. 65–70.
- [59] M. Agarwal and G. M. S. Srivastava, "A Cuckoo Search Algorithm-Based Task Scheduling in Cloud Computing," *Advances in Computer and Computational Sciences*, Springer, Singapore, 2018, pp. 293–299.
- [60] Sumandeep Aujla, Amandeep Ummat, "Task Scheduling in Cloud using Hybrid Cuckoo Algorithm", *International Journal of Computer Networks and Applications (IJCNA)*, Vol. 2, Issue 3, 2015, pp. 144–150.
- [61] Afroz moradbeiky, Vahid Khatibi Bardsiri, "A Novel Task Scheduling Method in Cloud Environment Using Cuckoo Optimization Algorithm", *International Journal of Cloud –Computing and Super-Computing*, Vol. 2, Issue 2, 2015, pp. 7–22.
- [62] M. Akbari and H. Rashidi, "A Multi-Objectives Scheduling Algorithm Based on Cuckoo Optimization for Task Allocation Problem at Compile Time in Heterogeneous Systems," *Expert Systems with Applications*, vol. 60, no. Supplement C, pp. 234–248, Oct. 2016.
- [63] X.-S. Yang, A New Metaheuristic Bat-Inspired Algorithm, in: *Nature Inspired Cooperative Strategies for Optimization (NISCO 2010)* (Eds. J. R. Gonzalez et al.), *Studies in Computational Intelligence*, Springer Berlin, 284, Springer, 65–74 (2010).
- [64] T. L. Best, "Altringham, J. D. 1996. *Bats: Biology and Behaviour*. Oxford University Press, Inc., New York, 262 pp. ISBN 0-19-854075-2, price (hardcover), \$65.00," *J Mammal*, vol. 78, no. 3, pp. 986–987, Aug. 1997.
- [65] Navneet Kaura, Sarbjee Singh, "A Budget-Constrained Time and Reliability Optimization BAT Algorithm for Scheduling Workflow Applications in Clouds", 7th International Conference on Emerging Ubiquitous Systems and Pervasive Networks", *Procedia* 98, pp. 199–204.
- [66] T Sunitha Rani, Dr. Shyamala Kannan, "Task Scheduling on Virtual Machines Using BAT Strategy for Efficient Utilization of Resources in Cloud Environment", *International Journal of Applied Engineering Research*, Vol. 12, Issue 17, pp. 6663–6669, 2017
- [67] S. Raghavan, P. Sarwesh, C. Marimuthu, and K. Chandrasekaran, "BAT Algorithm for Scheduling Workflow Applications in Cloud," 2015 International Conference on Electronic Design, Computer Networks Automated Verification (EDCAV), 2015, pp. 139–144.
- [68] Fereshteh Ershad Farkar, Ali Asghar Pourhaji Kazem, "Bi-Objective Task Scheduling in Cloud Computing Using Chaotic BAT Algorithm", *International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 10, pp. 223–229, 2017.
- [69] X. Huang, X. Zeng, and R. Han, "Dynamic Inertia Weight Binary BAT Algorithm with Neighborhood Search," *Computational Intelligence and Neuroscience*, Vol. 2017, pp. 1–15, 2017, doi:10.1155/2017/3235720

- [70] V Suresh Kumar, Aramudhan, "Trust Based Resource Selection in Cloud Computing using Hybrid Algorithm", International Journal of Computational Intelligence and Informatics, Vol. 4: No. 3, pp. 169-176, 2014.
- [71] E. Jafarnejad Ghomi, A. Masoud Rahmani, and N. Nasih Qader, "Load-Balancing Algorithms in Cloud Computing: A Survey," Journal of Network and Computer Applications, vol. 88, no. Supplement C, pp. 50-71, Jun. 2017.
- [72] B. Raj, P. Ranjan, N. Rizvi, P. Pranav and S. Paul, "Improvised BAT Algorithm for Load Balancing Based Task Scheduling," Advances in Intelligent System and Computing, vol. 518, pp. 521-530, 2018.
- [73] A. M. Manasarh and H. Ali, "workflow Scheduling Using hybrid GA-PSO in Cloud Computing," Wireless Communications and Mobile Computing, vol. 2018, pp. 1-16, 2018.

Selecting Prominent API Calls and Labeling Malicious Samples for Effective Malware Family Classification

Cho Cho San¹ and Mie Mie Su Thwin²

^{1,2}Cyber Security Research Lab, University of Computer Studies, Yangon, Myanmar

¹chochosan@ucsy.edu.mm

²drmiemiesuthwin@ucsy.edu.mm

Abstract- Today's threats have become very complex and serious in their packing and encryption techniques. Every day new malware variants are becoming increasingly in quantity together with quality by using packing and encrypting techniques. The challenges in this research field are the traditional malware detection systems sometimes might fail to detect new malware variants and produces false alarms. Malicious software in the form of virus, worm, trojan, ransom, and spy harms our computer systems, network environment, and organizations in various ways. Therefore, malware analysis for detection and family classification plays a significant role in Cyber Crime Incident Handling Systems. This system contributes malware family classification with 10 prominent features by conduction feature selection process. The process of labeling the malicious samples using Regular Expressions has been contributed in this approach. The proposed malware classification system provides 7 different families including malware and benign using machine learning classifiers. The finding from our experiment proves that the selected 10 API features provide the best evaluation metrics in terms of accuracy, precision-recall, and ROC scores.

Keywords - Malware analysis, Malware classification, Feature selection, Regular Expressions, Machine learning, API calls

I. INTRODUCTION

The sophisticated and advanced threat actors, Advanced Persistent Threats (APT), are targeted attack and the threat actor can hide persistently in target network or computer until their mission accomplished. The destructive malware attacks are happening due to the weakness of network security, lack of software updating or patching, and lack of employee awareness. A single malicious software can attack and infect thousands or even millions of computers in various ways simultaneously. New malware variants are becoming increasingly in million number including viruses, worms, ransomware, adware, spyware, and trojan horses. The most common malware that can be found in the wild is trj called Trojan.

Recently, due to the fastest growth of the internet, information technologies and smart devices, the harmful types of malware are increasing. The malwares are increasing rapidly every year, so it is very essential to detect the malwares in the system. Because it can easily damage the system and reduce overall performance. Malware analysis and classification are also important in the modern malware detection system to reduce and prevent cybercrimes. It is not new, but still needs to focus on cyber-security, so many researchers are interested in analyzing and classifying the variants of malware using the Windows API (Application Programming Interface) according to the sequence of modern malware behavior through static or dynamic analysis.

The behaviors of malware can be constructed from the API information by applying static (no action to execute the malware) and dynamic (run the malware in a safe environment) analysis approaches. In [1], the authors discussed two ways to analyze the API calls collected via the static approach such as counting the APIs called frequency and applying data mining methods or machine learning to these captured APIs. These API can also be

used for creating behavioral patterns in dynamic analysis with these two ways. In [1] the authors also discussed dynamic analysis has two major approaches which are control flow and API call analysis.

The malicious program is becoming increasingly destructive for both end users and government/non-government organizations. That's why we conduct the malware family classification research on this area by conducting the dynamic analysis. In our approach, we perform dynamic malware analysis on API call using cuckoo sandbox [28] and malware executable files are obtained from the virus share [30]. The purpose of our proposed work highlights as followed:

- 1) To analyze the nature and variations of malware,
- 2) To identify the important features of malware using their data access patterns,
- 3) To extract the API calls, and select the prominent APIs
- 4) To classify the malware files with their families from benign samples

The API calls are extracted and stored the sequence of unique API calls for each executable. We pinpoint the extracted 306 API features from different categories such as network, system, file, process, and registry can provide the accuracy in the testing dataset with 94.8% accuracy using the Random Forest (RF) classifier. Moreover, we apply the n-gram ($n = 1, 2$) on the API function calls because the importance of malicious behaviors not only depends on the frequency but also depends on the sequence of API before and after they called. So, this system uses 1-gram and 2-gram API call sequences from extracted API attributes. Then feature selection methods such as Chi-Square, Kernel Principal Component Analysis (KPCA), and Principal Component Analysis (PCA) from sci-kit learn [27] apply on both 1-gram (306 APIs) and 2-gram (10796 APIs) to select the most importance API features and including runtime for classification. As we concern the low computational complexity in this system, so n-gram ($n = 1, 2$) only considered in the experiments. The 3-gram or 4-gram features could lead to a larger number of APIs, and the run time duration required to select and classify those features will take more time than normal.

Section 2 discusses the recent work of malware feature selection methods and malware family classification system; the proposed system describes in Section 3. Section 4 highlights the results and discussion, and Section 5 concludes the system and supports future work.

II. RELATED WORK

This section describes some of the recent techniques and approaches for malware feature (API) selection methods in previous research works. And it also highlights the classification and detection of the malicious samples based on the extracted API calls. In [3] the authors used the ReliefF technique to reduce the features from 2188 features to 410. They got the accuracy 98.4% for 2188 features and 97.4% for selected ReliefF features. However, they tested on a small number of samples.

In [4], they analyzed the static and dynamic data extracted from malicious and benign in order to predict a test dataset. Feature Selection ChiSqSelector was applied to get the most relevant features. They applied the Random Forest on RStudio was also applied to select the best features from the previous feature selection result. Due to the unbalanced data, the oversampling was used and thus the new amount of observations was 14902. Three classification algorithms were used in their system. Their approach provides 99.60% accuracy with selected 9

features. In our approach, we also use Chi2 from sklearn for feature selection and it provides better accuracy than the other research works.

In [5] Tf-idf was used to reduce the time cost of classification. The PCA and KPCA methods were used to extract malware behaviors. Furthermore, they proposed a multi grouping algorithm. To reduce the time cost, the authors used the combination of multi grouping tf-idf and feature extraction methods by forming a two stage feature reduction method. In [7], the authors constructed n-grams ($n=96$) for each sample. They used the Information Gain by selecting the topmost 50,000 attributes. They also applied CfSubsetEval from Weka on the best 10,000 features to 29 best features. Their approach was shown better accuracy in a little family, while worse in others. In [6] they focused on the extraction of static malicious features for classification. They achieved accuracy nearly 0.998 on the Microsoft Malware Challenge dataset. The hex view and the assembly view representations were used in their paper. They described the representation of a malicious sample as a sequence of hex through n-gram analysis ($n = 1$). They used the combination of forward stepwise selection technique and best subset selection technique for feature fusion. However, the static approach faces the challenge of code evasion or encryption techniques.

In [8], the authors used static features as PE headers, DLLs and API functions, they selected the best subset of features consisting on 88 PE headers that had the performance with their classifiers (0.995 accuracy). However, static features are not convenient to detect malware files given that malware detection based on static features can be bypassed by obfuscation methods. In [9], the authors used 1,086 malwares from 7 classes and performed five-fold cross-validation for the evaluation. The precision of the Decision Tree and SVM are 83.60%, and 88.30% respectively.

The authors applied six different classification methods using the WEKA tool. They showed that the classification via regression provided the best evaluation result in malware detection. The correctly classified instance number is 75.8201% in 4024 malicious software for the first dataset. The correctly classified instance number is 98.321% for 3131 malware dataset 2. They tested 100 malware programs by adding to the new data set and compute the quality of their classification as a true optimistic ratio. A total of 88 malware programs were detected by using classification via regression [10]. The authors reduced from 7,605 features to 1,000 by using Information Gain (IG). They obtained accuracy 94.6% on the selected feature for the malware versus clean ware test and 94.5% on the malware classification test with Random Forest classifier [11].

In [12], they collected over 65,500 features from static analysis and applied InformationGain to discriminate these features. They formed 5 different attribute sets and used WEKA was used to train them. The 250 features set supported 98% classification accuracy. In our system, the Chi-Square feature selection method provides better accuracy than their work on the n-gram dataset using three machine learning classifiers such as Support Vector Classification (SVC), Random Forest and K-Nearest Neighbor.

III. THE PROPOSED SYSTEM

Nowadays, malware and Advanced Persistent Threats protection are more important than ever since cybersecurity threats and cyber-crimes are becoming increasingly. As long as malware evading technologies are increasing such as packing and encrypting to evade current antivirus software, further research to defense these kinds of attacks are essential in cybersecurity. Malware analysis, classification, and detection are important for becoming increasingly

targeted malware attacks. Therefore, this system provides the malware classification from benign and other families by extracting and selecting prominent malicious API features from dynamic analysis using Support Vector Classification (SVC), Random Forest (RF), and k-Nearest Neighbor (kNN) classifiers. These are implemented using the scikit-learn of Python machine learning library [27]. We contribute the right choice of malicious family labeling and prominent API feature selection in this paper. The proposed malware family classification system describes details in Figure 1. The proposed system contains 6 phases: A) collecting and analyzing malicious samples, B) preprocessing C) extracting API attributes from analysis's reports, D) postprocessing, E) selecting the significant API features, and F) classifying the executable using machine learning.

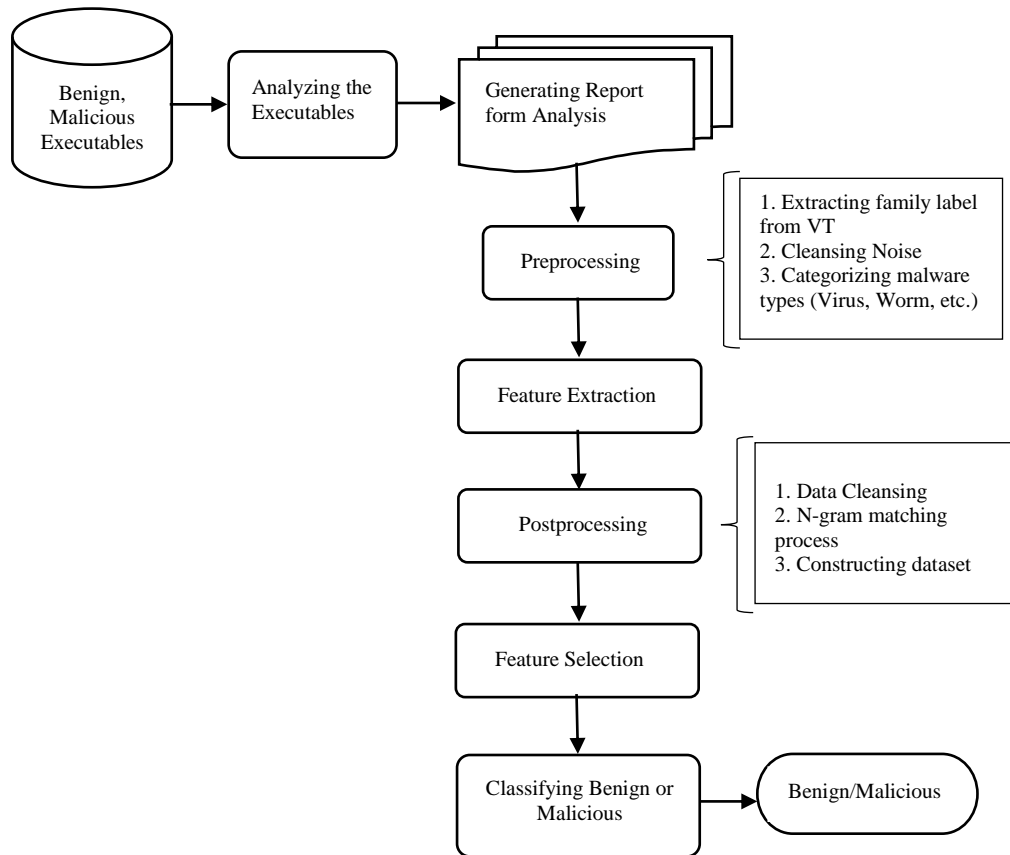


Figure 1. The proposed system

3.1 Gathering Samples and Performing Dynamic Analysis

We collected malicious samples from virusshare and tested over 20000 malwares in the experiment. The number of 15389 from 6 malware families and 5420 cleanware have experimented. Cuckoo Sandbox has been used for dynamic analysis and the Windows 7 32-bit operating system (OS) has been used to analyze the malware sample in VirtualBox and Ubuntu as host OS. Table 1 shows the tested samples per family and describes together with class labels. The cuckoo sandbox has been used to conduct dynamic analysis and it produces the HTML, JSON (Java Script Object Notation) reports. JSON has been used in this system to extract the APIs. The report contains the name/label of the sample from many antiviruses using VirusTotal.

TABLE I
TOTAL SAMPLES PER FAMILY IN THE EXPERIMENT

Label	Family	Number of Samples	Label	Family	Number of Samples
0	Clean	5420	4	Virus	1740
1	Adware	2200	5	Worm	2397
2	Backdoor	2076	6	Trojan	5000
3	Downloader	1976	Total number of samples		20809

3.2 Preprocessing

The preprocessing phase performs two main parts such as extracting the name of the malicious sample provided by VirusTotal and categorizing the malware family by using the most common name used by multiple antivirus vendors. The contribution of choosing the suitable family name or label exists in this phase of the proposed approach. As the new variants of malicious executable files are increasing, there is a conflict between the antivirus vendors to name the samples, for example, one malicious file has a different label or family name as trojan or adware or spyware or downloader. So, we contribute to extract the name or label based on their highest score of the sample's name provided by VirusTotal (VT) using Regular Expressions (RE). RE is a useful pattern matching techniques for characters, or fail to match, sequences of characters in the text. It allows the developers and users to find desired characters or words and to replace these characters with something that the users preferred [34]. Figure 2 shows the procedure of extracting the VT labels from reports. According to the analysis report files, the labels of samples can get by using the keyword "result" from cuckoo JSON.

VT Labels Extraction Procedure

Input: JSON reports

Output: extracted family labels text files f_i

```

1: begin
2:   if (JSON ≤ JSONs)
3:     for line in JSON
4:       result = line.find ("\"result\":")
5:       vt_result = line[result:]
6:       print (vt_result)
7:     end for
8:   end if
9: end

```

Figure 2. Procedure for VT Results Extraction

After processing the VT label extraction, raw data cleaning has been performed in the proposed system. All unnecessary data have been removed using the following steps as conditionally:

1. Remove the empty line, if there is an empty line
2. Get the VT label data
3. Remove all noise data
4. Keep the rest in raw labels files

Then the family label name extraction has been carried out by depicting the Figure 3. RE has been used in this proposed system to choose the family of malicious programs and the number of characters for the sample's name is limited to 3 to 15 word. After applying the RE, the number of word or frequency of word found in the raw labels' files are stored in an array. And then sorting step is performed and choice the highest labels name from them. The example of the sample's label result from the RE technique is shown in Figure 4. It describes the count and sample name of the single executable file from VT results. According to this text file result, the proposed system noted that this sample belongs to the trojan family.

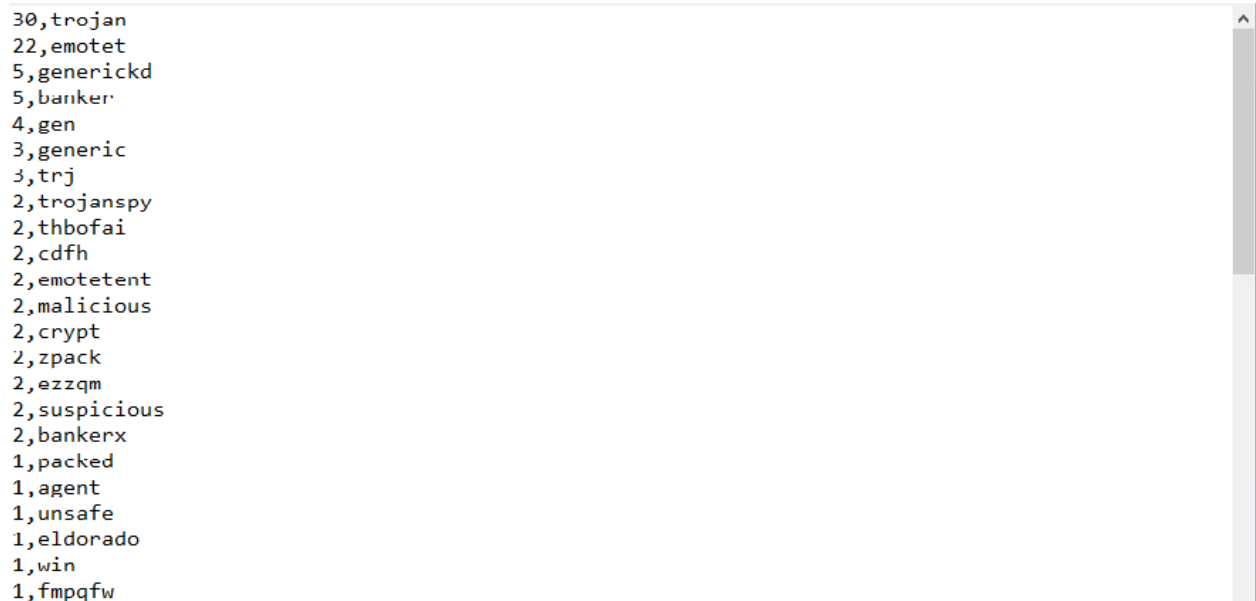
Labelling the malicious samples by using RE technique

Input: raw labels files l_i

Output: family labels for malicious samples

```
1: begin
2:   frequency = { }
3:   if ( $1 \leq l_i$ )
4:     match = re.findall(r"[a-zA-Z]{3,15}\b", l)
5:     while (word  $\in$  match)
6:       count = frequency[word], 0
7:       frequency[word] = count+1
8:       frequency_list = frequency.keys()
9:       while (words  $\in$  frequency_list)
10:        count_word = frequency[words], words
11:        print (count_word)
12:        sort the count_word to get the highest majority score of VT name
13:        choose the max_number of words as labels
14:      end while
15:    end while
16:  end if
17: end
```

Figure 3. Malicious samples labeling using RE technique



```
30,trojan
22,emotet
5,generickd
5,banker
4,gen
3,generic
3,trj
2,trojanspy
2,thbofai
2,cdfh
2,emotetent
2,malicious
2,crypt
2,zpack
2,ezqzm
2,suspicious
2,bankernx
1,packed
1,agent
1,unsafe
1,eldorado
1,win
1,fmpqfw
```

Figure 4. Labels for malicious sample using RE

Then we categorize the sample into their corresponding family. The key role is to find the family label that gives both the best detection rate and the most precise labeling [31]. This proposed system performs malware classification from benign with 7 different families such as Clean, Adware, Backdoor, Downloader, Virus, Worm and Trojan.

3.3 Extracting API Features

The API features (categories from network, system, file, process, and registry) are extracted by using our proposed malware feature extracting algorithm in our previous research work [13]. The API features are extracted according to the called API by malware. The number of APIs called by malware is quite large to handle the classification and irrelevant features might lead to failing the detection and it can also increase the false positive rate (FP), and false negative rate (FN).

3.4 Postprocessing

The postprocessing phase contains three steps removing duplicate and noise API calls, applying n-gram, and constructing the dataset for malicious-benign classification. The total number of API features are 306, after the data cleaning process. It is not quite large to classify malware family in terms of processing time and performance. However, malicious features are correlated with each other sequentially according to their API categories e.g. NtClose (system), NtOpenKey (registry), NtQueryValueKey (registry), NtQueryAttributesFile (file). Therefore, the n-gram method is applied in this system to find the correlated API calls and to improve the classification performance. N-gram is an efficient method for text feature extraction, where n denotes the length of the feature. The length determines the performance of the algorithm. Therefore, in this approach, we employ two different lengths to API calls in three classification algorithms. As shown in Table 3, n-gram (n=2) provides the best accuracy on all classifiers. In [14, 15, 16, 17], n-gram was applied in their works but most of the methods that used n-gram are based on static features. In this paper, a new API call sequence processing method is proposed for malware family and benign classification. As we concern the low computational complexity and 2-gram provides the best accuracy, we use n-gram with (n = 1,2). The total number of 1-gram API features are 306 grams and 2-gram API features are 10796 grams. We use one hot encoding technique to construct the dataset which simply takes a mapping transformation to get a sparse vector like [1, 0, 0, 1, 0, ..., 0].

3.5 Selecting API Features

Selecting an important attribute is one of the essential techniques in data mining especially during the data processing. The main role of this phase is to improve the classification performance as well as improving the detection accuracy by removing the noisy attribute, redundant, and irrelevant from the dataset. The aim of this paper is to find the best API features which can provide to improve the classification rate of malicious and benign executables and to decrease the FP and FN. To remove the irrelevance features in classification, this research investigates three different feature selection methods. The machine learning library for sklearn has been used for feature selection. Chi-squared test (or χ^2 test), Principal Component Analysis (PCA), Kernel Principal Component

Analysis (KPCA) methods are applied to select the discriminate API call features. We experiment with different numbers of samples 10,25,50,150 API features using three selection methods.

3.5.1 *Chi-squared*

The Chi-squared method evaluates features individually by measuring their chi-squared statistic with respect to the classes. For a numeric attribute, the method first requires its range to be discretized into several intervals using, for example, the entropy-based discretization method [18]. The formula for computing the χ^2 value can be found in [19]. In [4,32], they also used the χ^2 method to select features.

3.5.2 *Principal Component Analysis (PCA)*

PCA is a popular dimensionality reduction technique. PCA is an orthogonal linear transformation that transforms the data to a new coordinate system such that the greatest variance by any projection of the data comes to lie on the first coordinate (called the first principal component), the second greatest variance on the second coordinate, and so on [33]. It is widely used in image processing and attribute extraction and reduction for malware detection in security [20,5]. In this experiment, PCA feature selection with a default setting of sklearn has been used.

3.5.3 *Kernel Principal Component Analysis (KPCA)*

In KPCA, through the use of kernels, principal components can be computed efficiently in high-dimensional feature spaces that are related to the input space by some nonlinear mapping. KPCA finds principal components that are nonlinearly related to the input space by performing PCA in the space produced by the nonlinear mapping, where the low-dimensional latent structure is, hopefully, easier to discover [22]. It is useful for image processing fields such as noise reduction, and for cybersecurity fields e.g. feature extraction and selection [20,5].

4 *Classifying Malicious Software from Benign*

Machine learning can be divided into supervised learning and unsupervised learning. The purpose of supervised learning is to obtain a correct output against the input data. On the other hand, the purpose of unsupervised learning is to find the regularity from input data [3]. For classification purpose, three different classifiers are used in this proposed system such as Random Forest (RF), k-Nearest Neighbor (k-NN) and Support Vector Classification (SVC) classifiers that can classify the multi-class in scikit-learn.

4.1 *Random Forest*

RF is an ensemble learning classifier and it can overcome the problems of overfitting and hence there is no need to prune the trees [4]. The value of n_estimators changes in our approach to 250.

4.2 *K-Nearest Neighbors*

Neighbors-based classification is an instance-based learning or non-generalizing learning: it does not attempt to construct a general internal model, but simply stores instances of the training data. Classification is computed from a simple majority vote of the nearest neighbors of each point: a query point is assigned the data class which has the most representatives within the nearest neighbors of the point. KNeighborsClassifier implements learning based on

the nearest neighbors of each query point, where is an integer value specified by the user [27]. In our approach, we use the value of $k = 3$ and the distance metric is MinkowskiDistance.

4.3 Support Vector Classification (SVC)

Support Vector Machines (SVMs) are a popular machine learning method for classification, regression, and other learning tasks. The authors developed a library for support vector machines, Libsvm package. Libsvm supports the Support Vector Classification (SVC) for two-class and multi-class [25]. The fit time complexity is more than quadratic with the number of samples which makes it hard to scale to a dataset with more than a couple of 10000 samples [27].

IV. EXPERIMENT RESULTS AND DISCUSSION

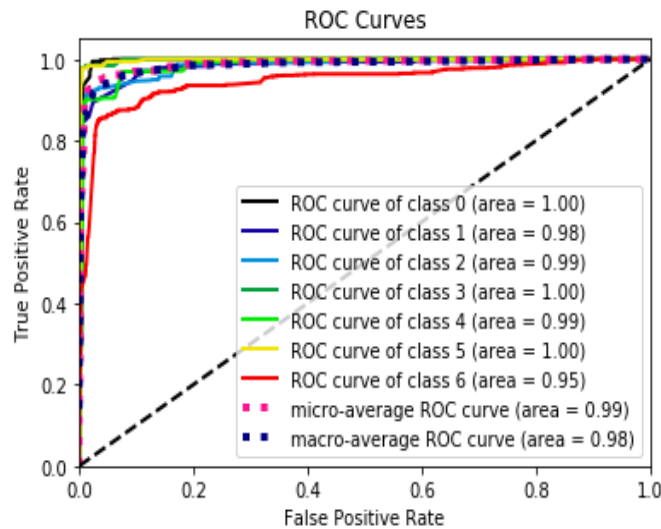
This system analyzed over 25000 executables from 7 families and including benign samples. However, we do not consider the case of evading from the analysis awareness of the virtual environment. After the malware execution, the next step is to extract the malware label from the report and categorize them to their family using the RE technique. And then extracted API from the report using our previously proposed feature extraction algorithm in [13]. Then we conducted data cleansing and implement n-gram on these API calls. Grams such as 1-gram, and 2-gram have been built, databases of API sequences as the training API database for 7 families. Then one-hot encoding has been used in this system to represent these APIs as 0 (absence) or 1 (presence) and feature selection has been performed. We experiment on four different number of features (10,25,50,150) with Chi2, PCA, KPCA feature selection methods. However, finding from our experiment is 10 features for 1-gram and 2-gram are enough to discriminate malicious from benign and other malware families. In [4], the authors also showed that 9 features were enough to detect malware from cleanware with an accuracy of over 99%. But our approach provides better accuracy than their work when Chi2 and SVC combine together. We split the 30% (6243 samples) of our API dataset for testing purposes and training for the rest 70%. The performance of a malware classification system is evaluated according to different metrics accuracy, precision-recall (PR) score and ROC scores using sklearn.

TABLE II
EXPERIMENT RESULTS ON TEST SET WITH OR WITHOUT FEATURE SELECTION ON 1-GRAM APIS

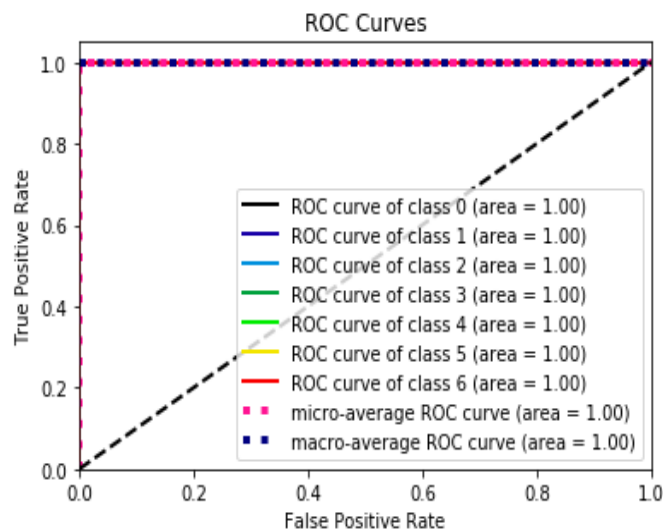
Classifiers	Without Feature Selection Test Accuracy (306 API)	Feature Selection Test Accuracy (10 API)		
		Chi2	PCA	KPCA
RF	0.948	0.999	0.943	0.944
SVC	0.918	1.0	1.0	0.65
KNN	0.915	0.999	0.905	0.948

Table 2 provides the experiment output of 1-gram for API dataset. The total number of test samples and API features are (6243, 306). Table 2 also compares the accuracies with or without feature selection and different feature selection methods. Chi2, PCA with SVC provides better accuracy 100 percentage than the others and without feature selection, RF supports the best accuracy with 0.948 in the test dataset. SVC with KPCA shows the worse in our test case.

Others prove that the selected 10 API features correctly predict the malware from benign and their families. The accuracy from RF also provides better than the others if feature selection is not performed. Figure 5 describes the ROC (receiver operating characteristic) Curves for SVC that provides better accuracy on test set than the other classifiers for feature selection methods Chi2 and PCA.



(a) SVC Without feature selection

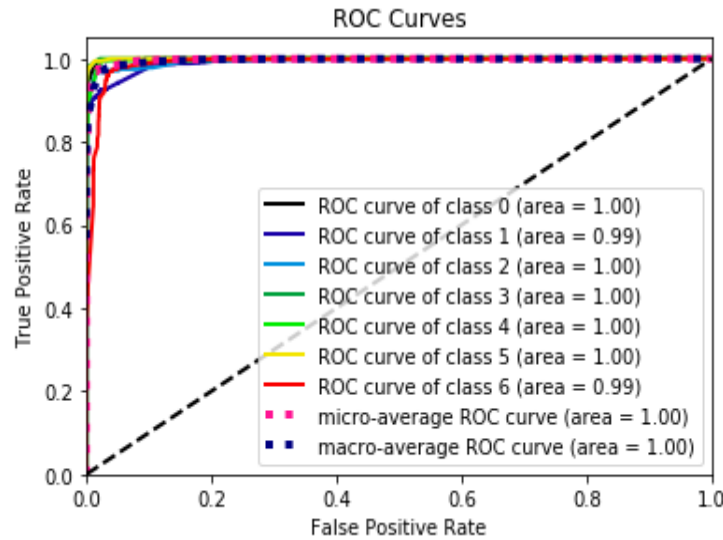


(b) SVC with Chi2

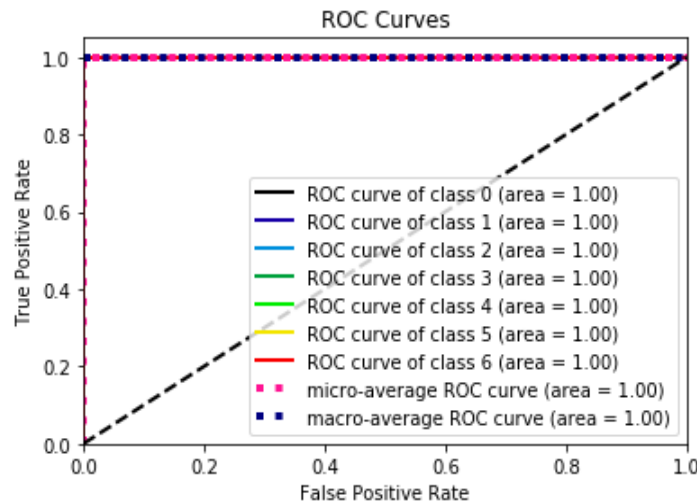
Figure 5. ROC curves for SVC on test dataset (1-gram)

The ROC curves for RF classifier also described in Figure 6. Figure 6 compares the evaluation results of before and after applying the feature selection methods. The extracted API features (306 APIs) show that it is enough to distinguish between malware and cleanware samples.

Some researches focus on the extracting of API functions that are frequently called and calculated the total number of functions called. But they failed to show the sequence of malware behavior and can be easily evaded when malware creators insert and execute dummy and redundant API calls [4]. In [1], the authors used API call sequences as features and got 0.998 accuracy in classification from benign and malware executables. DNA sequence alignment algorithm had been used for the detection of malware samples. In this approach, 2-gram API sequence alignment has been used for differentiating malware families and from benign.



(a) RF Without feature selection



(b) RF with Chi2

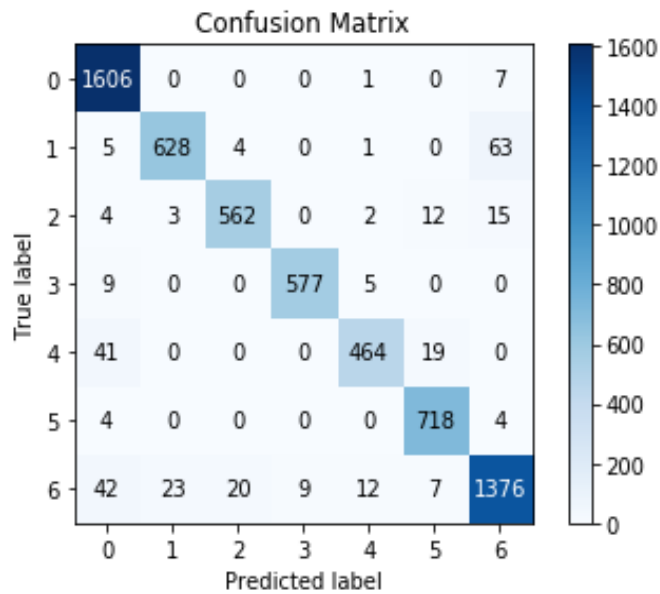
Figure 6. ROC curves for RF on test dataset (1-gram)

Table 3 shows the evaluation result of 2-gram test data on three different feature selection methods and classifiers. By using the Chi2 feature selection methods our system provides the best accuracy than the recent state-of-the-art approaches. Chi2 feature selection method gives the best 100% accuracy on three different classifiers and the selected 10 API features are enough to distinguish malware families and benign. PCA also produces the second-best evaluation result on the test dataset. KPCA does not support good accuracy on the SVC classifier but worth it on

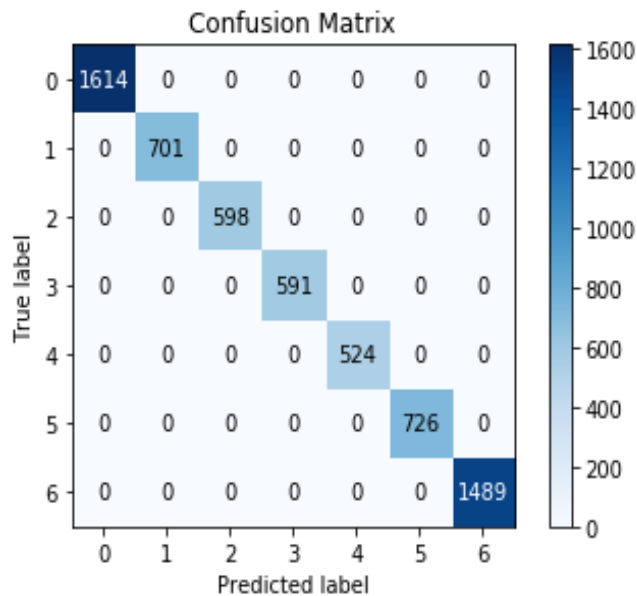
others. Figure 7 describes the confusion matrix (CM) of the test dataset for RF classifier before and after applying the feature selection technique.

TABLE III
EXPERIMENT RESULTS ON TEST SET WITH OR WITHOUT FEATURE SELECTION ON 2-GRAM APIS

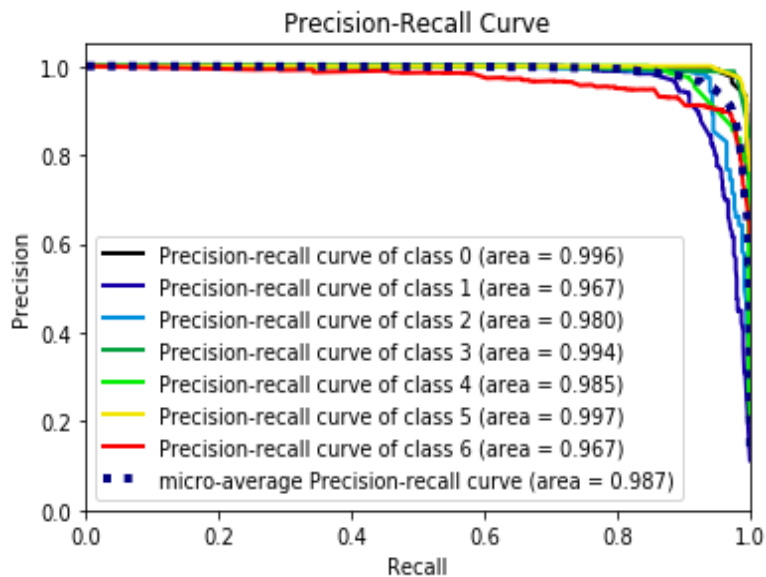
Classifiers	Without Feature Selection Test Accuracy (10796 API)	Feature Selection Test Accuracy (10 API)		
		Chi2	PCA	KPCA
RF	0.95	1.0	0.949	0.949
SVC	0.933	1.0	0.997	0.614
KNN	0.906	1.0	0.904	0.934



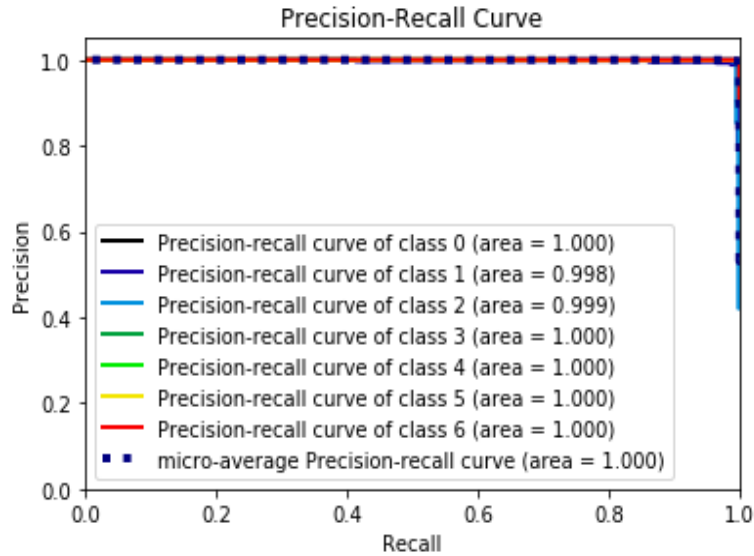
(a) CM before selecting feature



(b) CM with Chi2
Figure 7. CM for RF classifier on 2-grams

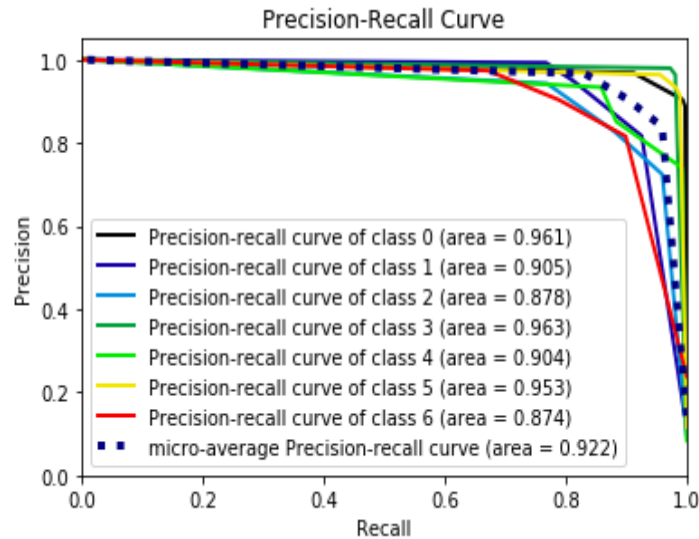


(a) PR curve for RF



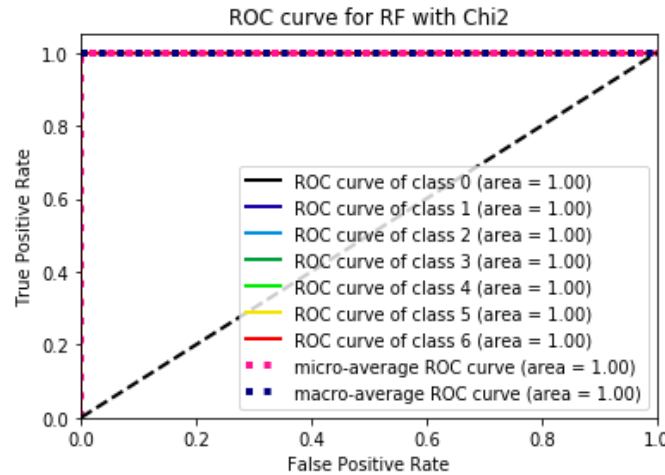
(b) PR curve for SVC

Figure 8 shows the precision-recall curves of PCA on testing dataset 6243 samples and 10 API features. SVC provides better performance results on test data by using the PCA method but not for KPCA. It takes more time than the other classifiers during training and testing. However, the time consuming reduces significantly after applying the feature selection methods, just hour to minutes. The ROC and Precision-recall curves for RF classifier with Chi2 are shown in Figure 9. RF classifier supports better accuracy among three classifiers before applying feature selection methods on both 1-gram and 2-gram dataset.

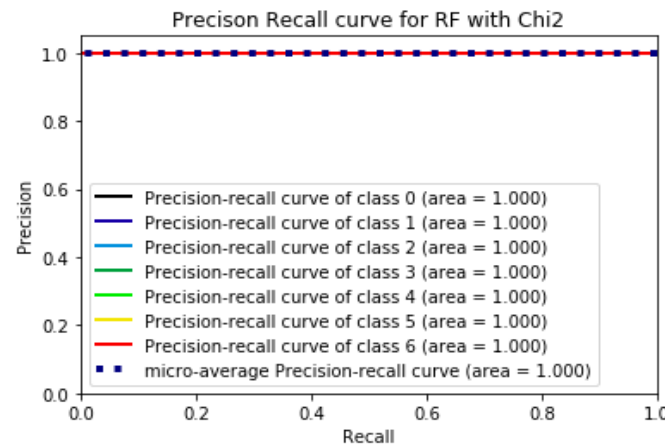


(c) PR curve for k-NN

Figure 8. Precision-recall curves of PCA on 2-grams



(a) ROC curve for RF



(b) Precision-recall curve for RF

Figure 9. ROC and PR curves for RF on 2-grams with Chi2

IV. CONCLUSION

The proposed system contributes malware family classification using API call sequence on n-gram through dynamic analysis. Labeling the malicious samples using the RE technique has been contributed in the proposed system. The proposed system classifies malware based on 7 different families by 3 machine learning classifiers. This paper applies feature selection algorithms Chi2, PCA and KPCA to remove irrelevant or noise features and then to select dominant features. These main features help to identify the new unknown variants of malicious behaviors in real-world applications. The result shows that selected prominent API features achieve the best accuracy of 100% on all classifiers with the Chi2 feature selection method in our experiment. The performance evaluation metrics, ROC and Precision-recall scores, are higher than the recent previous research works. The key components of the proposed system compose of extracting the malware samples name from VirusTotal and labeling and categorizing these samples by using regression regular expression theory, applying the n-gram sequence on extracted API calls in postprocessing and selecting the most important API features from the n-gram API sequences. Ngram ($n = 1, 2$) use in the proposed system because of the concern of processing time when 3-gram and 4-gram features lead to a larger

number of API components. Moreover, 2-gram API call sequences are enough to detect and classify malicious behaviors using χ^2 feature selection method. The proposed system provides the best performance metrics than previous research works.

Therefore, the experiment shows that the proposed system provides the best performance with low FP and FN rates. And it can classify malware based on their relevant families by selecting prominent API features from dynamic analysis reports. The proposed system contributes important API feature selection and correct family labeling for classification. By extending the current work, we will perform to detect the unknown malware and zero-day attacks detection system in future work.

ACKNOWLEDGMENT

I would like to thank all the reviewers for their precious comments.

REFERENCES

- [1] Y. Ki, E. Kim, & H. K. Kim, "A novel approach to detect malware based on API call sequence analysis", *International Journal of Distributed Sensor Networks*, 11(6), 659101, 2015.
- [2] M. Rajagopalan, M. A. Hiltunen, T. Jim, & R. D. Schlichting, "System call monitoring using authenticated system calls", *IEEE Transactions on Dependable and Secure Computing*, Vol. 3, No. 3, pp216-229, 2006.
- [3] Z. Salehi, M. Ghiasi, & A. Sami, "A miner for malware detection based on API function calls and their arguments", In *The 16th CSI International Symposium on Artificial Intelligence and Signal Processing (AISP 2012)*, pp563-568, IEEE, May 2012.
- [4] C. Cepeda, D. L. C. Tien, & P. Ordóñez, "Feature selection and improving classification performance for malware detection", In *2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom)(BDCloud-SocialCom-SustainCom)* pp560-566, IEEE, October 2016.
- [5] C. T. Lin, N. J. Wang, H. Xiao, & C. Eckert, "Feature Selection and Extraction for Malware Classification", *J. Inf. Sci. Eng.*, 31(3), pp965-992, 2015.
- [6] M. Ahmadi, D. Ulyanov, S. Semenov, M. Trofimov, & G. Giacinto, "Novel feature extraction, selection and fusion for effective malware family classification", In *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, pp183-194. ACM, March 2016.
- [7] S. Banin, & G. O. Dyrkolbotn, "Multinomial malware classification via low-level features", *Digital Investigation*, 26, ppS107-S117, 2018.
- [8] U. Baldangombo, N. Jambaljav, & S. J. Horng, "A static malware detection system using data mining methods", *arXiv preprint arXiv:1308.2831*, 2013.
- [9] J. Hong, S. Park, & S. W. Kim, "On exploiting static and dynamic features in malware classification", In *International Conference on Big Data Technologies and Applications*, pp122-129, Springer, Cham, November 2016.
- [10] M. Norouzi, A. Souri, & M. Samad Zamini, "A data mining classification approach for behavioral malware detection", *Journal of Computer Networks and Communications*, 2016, pp1, 2016.
- [11] V. Moonsamy, R. Tian, & L. Batten, "Feature reduction to speed up malware classification", In *Nordic Conference on Secure IT Systems*, pp176-188, Springer, Berlin, Heidelberg, October 2011.
- [12] D. Komashinskiy, & I. Kotenko, "Malware detection by data mining techniques based on positionally dependent features", In *2010 18th Euromicro Conference on Parallel, Distributed and Network-based Processing*, pp617-623, IEEE, February 2010.
- [13] C. C. San, M. M. S. Thwin, & N. L. Htun, "Malicious Software Family Classification using Machine Learning Multi-class Classifiers", In *Computational Science and Technology: 5th ICCST 2018, Lecture Notes in Electrical Engineering*, vol 481, pp423-433, Springer, Singapore, August 2018.
- [14] L. Liu, B. S. Wang, B. Yu, & Q. X. Zhong, "Automatic malware classification and new malware detection using machine learning", *Frontiers of Information Technology & Electronic Engineering*, Vol.18, No.9, pp1336-1347, 2017.
- [15] M. M. Masud, L. Khan, & B. Thuraisingham, "A hybrid model to detect malicious executables", In *2007 IEEE International Conference on Communications*, pp.1443-1448, IEEE, June 2007.
- [16] J. Z. Kolter, & M. A. Maloof, "Learning to detect malicious executables in the wild", In *Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining*, pp470-478, ACM, August 2004.
- [17] A. Kapoor, & S. Dhavale, "Control flow graph based multiclass malware detection using bi-normal separation", *Defence Science Journal*, Vol. 66, No. 2, pp138-145, 2016.
- [18] H. Liu, J. Li, & L. Wong, "A comparative study on feature selection and classification methods using gene expression profiles and proteomic patterns", *Genome informatics*, 13, pp51-60, 2002.
- [19] H. Liu, & R. Setiono, "Chi2: Feature selection and discretization of numeric attributes", In *Proceedings of 7th IEEE International Conference on Tools with Artificial Intelligence*, pp388-391, IEEE, November 1995.
- [20] M. Palechor, F. Enrique, A. K. De La Hoz Manotas, E. De La Hoz Franco, & P. P. Ariza Colpas, "Feature selection, learning metrics and dimension reduction in training and classification processes in intrusion detection systems", 2015.
- [21] V. Lohweg, & U. Mönks, "Fuzzy-pattern-classifier based sensor fusion for machine conditioning", In *Sensor Fusion and its Applications*, IntechOpen, 2010.
- [22] A. Ghodsi, "Dimensionality reduction a short tutorial", Department of Statistics and Actuarial Science, Univ. of Waterloo, Ontario, Canada, 37, pp38, 2006.
- [23] D. Adachi, & K. Omote, "A host-based detection method of remote access trojan in the early stage", In *International Conference on Information Security Practice and Experience*, pp110-121, Springer, Cham, November 2016.
- [24] Y. Qi, "Random forest for bioinformatics", In *Ensemble machine learning*, pp.307-323, Springer, Boston, MA, 2012.

- [25] C. C. Chang, & C. J. Lin, "LIBSVM: a library for support vector machines", *ACM transactions on intelligent systems and technology (TIST)*, Vol. 2, No. 3, pp27, 2011.
- [26] R. Tian, R. Islam, L. Batten, & S. Versteeg, "Differentiating malware from cleanware using behavioural analysis", In 2010 5th international conference on malicious and unwanted software, pp23-30, IEEE, October 2010.
- [27] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, & J. Vanderplas, "Scikit-learn: Machine Learning in Python," *Journal of machine learning research*, Vol. 12, pp2825–2830, 2011.
- [28] C. Guarnieri, A. Tanasi, J. Bremer, & M. Schloesser, *The cuckoo sandbox*, 2012.
- [29] V. Total, "Virustotal-free online virus, malware and url scanner", Online: <https://www.virustotal.com/en>, 2012.
- [30] VirusShare, [online] Available: <http://tracker.virusshare.com:6969/>
- [31] R. S. Pircoveanu, S. S. Hansen, T. M. Larsen, M. Stevanovic, J. M. Pedersen, & A. Czech, "Analysis of malware behavior: Type classification using machine learning", In 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp.1-7, IEEE, June 2015.
- [32] M. Belaoued, & S. Mazouzi, "A Chi-Square-Based Decision for Real-Time Malware Detection Using PE-File Features", *Journal of Information Processing Systems*, Vol.12, No.4, pp.644~660, 2016.
- [33] Wasuta. Renkjunong, "SVD and PCA in Image Processing", Thesis, Georgia State University, https://scholarworks.gsu.edu/math_theses/31, 2007.
- [34] A.Watt, *Beginning regular expressions*. John Wiley & Sons, 2005.

Text Extraction System by Eliminating Non-Text Regions

S.Shiyamala¹, S.Suganya²

¹Department of Computer Science, Rathnavel Subramaniam College of Arts and Science,
Coimbatore, TN, India

²Department of Computer Science, Rathnavel Subramaniam College of Arts and Science,
Coimbatore, TN, India

E-mail: shiyam05@gmail.com, sugan_senthil@yahoo.co.in

Corresponding Author: shiyam05@gmail.com Tel : 9487523134

ABSTRACT

Text detection and recognition in scene images or natural images has applications in computer vision systems like registration number plate detection, automatic traffic sign detection, image retrieval and help for visually impaired people. Scene text, however, has complicated background, blur image, partly occluded text, variations in font-styles, image noise and ranging illumination. Hence scene text recognition could be a difficult computer vision problem. In this paper connected component method is used to extract the text from background. In this work, horizontal and vertical projection profiles, geometric properties of text, image binarization and gap filling method are used to extract the text from scene images. Then histogram based threshold is applied to separate text background of the images. Finally text is extracted from images.

Keywords : Horizontal and vertical projection, Geometric properties of text, Image binarization and Gap filling method

I. INTRODUCTION

In the recent years, the world has seen the image and video capturing technologies grow exponentially. Few examples include digital cameras, mobile phones, etc. With the improvisation in image capturing devices and their ease of use, there is being captured and stored, which may contain useful data. The challenge that remains in front of us is that of processing these images to bring out the required detail. One appealing and developing field comprises of extracting the text from images. Digital image processing is used for extracting the text from image. "Image processing is the study of algorithm that takes image as input and returns an image as output". Images with text have various complexities that arise due to real world backgrounds, font sizes, and text positioning and so on. In some cases, low quality of capturing devices adds another level of difficulty. Existing methodologies for text extraction include region based, connected component based, texture based. Region based method used gray scale properties to differentiate text from background, whereas texture based method uses textual properties.

There are many hurdles or problems in detection of text, extraction of text and localization of text from images. In the proposed work, in order to overcome all these hurdles and problems that are occur when extracting text from images, texture - based method used in this proposed scheme. In this, image is converted into black and white image and used the filter to remove noises and used morphological operations for the feature extraction from image and for extracting the text from image discrete wavelet transform is used. The implementation of the following work would prove useful in solving real world problems such as license plate capturing of speeding vehicles, translation of sign/board, capturing city maps, to capture directive of the routes, to capture public notice and to capture advertisement banners etc. All these images contain useful and important information. And this information present in the images is used in the variety of applications.

II. RELATED WORK

Existing text - detection methods can be divided into region based and texture based methods. Region based methods rely on image segmentation. Pixels are grouped to CCs which are character candidates. These candidates are further grouped to candidate words and textlines based on geometric features. Texture based methods distinguish text from non-text based on local features and machine learning techniques.

Chen et al. [4] propose a text detection method using MSER. The outlines of MSER are improved by edges detection techniques such as canny edge detection. This makes MSER less responsive to blur images. Based on geometric cues these candidate character regions are then grouped to words and textlines.

Neumann et al.[3] propose ERs for segmenting regions. ERs are extracted on the gradient images, HSI and RGB to recover regions for character candidate. As an alternative of using heuristics as Epshtein et al. [3] for labeling text, an AdaBoost classifier based on geometric features is used. Text-CCs are then grouped to words.

Kim et al. [1] combined a Support Vector Machine (SVM) and continuously adaptive mean shift algorithm (CAMSHIFT) to detect and identify text regions. Gao et al. [9] developed a three layer hierarchical adaptive text detection algorithm for natural scenes. This method was applied in a prototype Chinese sign translation system which mostly has a horizontal and/or vertical alignment.

In Zheng et al.[7] proposed a completely unique image operator is projected to observe and find text in scene images to attain a high recall of character detection, extremal regions are detected as character candidates. 2 classifiers are trained to spot characters, and a algorithmic native search algorithm is projected to extract characters that are incorrectly known by the classifiers. An efficient pruning technique, which mixes component trees and recognition results, is projected to prune continuation elements. A cascaded technique combines text line entropy with a Convolutional Neural Network model. It's wont to verify text candidates that reduce the quantity of non-text regions. The projected technique is taking a look at on 3 public datasets, i.e. ICDAR2011 dataset, ICDAR2013 dataset and ICDAR2015 dataset.

Wang et al. [6] propose HOG features with a Random Ferns classifier to detect and classify text in an end to end setting. Multiclass detector is trained on letters. Non-maxima of the detector results are concealed. The remaining letters are then combined in a Pictorial Structure framework, where letters are parts of words. For each word in a dictionary, the most plausible character responses are found in the image. Detected words are then rescored based on geometric information and non-maxima suppression is done to remove overlapping word-responses.

In Greenhalgh et al.[2] proposed a unique system for the automated detection and recognition of text in traffic signs. Scene structure is employed to describe search regions at intervals the image,surrounded by traffic sign candidates are then found. Maximally Stable Extremal Regions (MSERs) and hue, saturation, and worth color thresholding are used to locate a large range of candidates, that are then reduced by applying constraints supported temporal and structural data. A recognition stage interprets the text contained at intervals detected candidate regions. Individual text characters are detected as MSERs and are classified into lines, before being interpreted using optical character recognition (OCR).

In Raj et al.[5] proposed connected component approach for extracting devanagiri text. But extraction accuracy is immensely improved through the temporal fusion of text results across consecutive frames.

III. PROPOSED METHOD

The common OCR systems available require the input image to be such that the characters can be easily parsed and recognized. The text and background should be monochrome and background-to-text contrast should be high. The proposed system briefly shows in Fig.1.

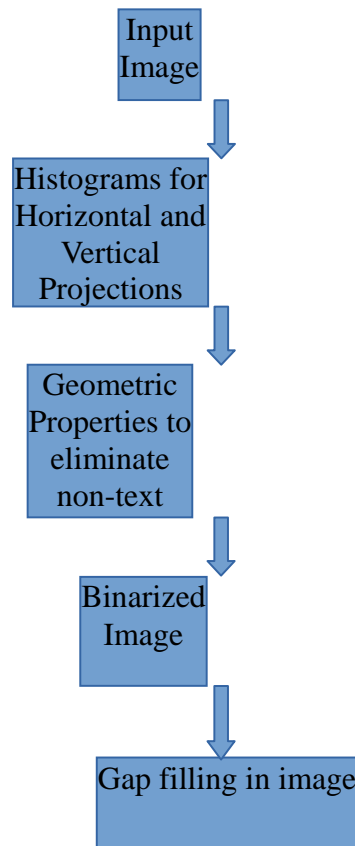


Fig.1: Flowchart of proposed system

The steps of the connected-component text extraction algorithm are given below,

- 1.The horizontal and vertical projection profiles of candidate text regions using a histogram with an appropriate threshold value.
2. Use geometric properties of text such as width to height ratio of characters to eliminate possible non-text regions.
3. Binarize the edge image enhancing only the text regions against a plain black background.
4. Morphological dilation is using the gap-filling process.

1.Horizontal and vertical projection using histogram

Projection profile of an image in a particular direction refers to the running sum of the pixels in that direction.In context of text processing, horizontal projection profile is needed to identify or

separate out the lines of a text since, the profile exhibits valley points at line boundaries and the location of these minima points mark the line boundaries.

Similarly, vertical projection profile is used to perform word segmentation as the valleys are created corresponding to word gaps. These word boundaries can be identified with the help of these minima points. Threshold selection is made by using the average value of maximum and minimum value of the corresponding projection is taken.

2. Eliminate non text regions

To improve the performance of the system, non text regions are eliminated using some rules according with text properties.

The rules are,

1. Text are limited in size.
2. Text must contain edges.
3. Text have special texture properties

3. Enhancing non text regions

Binirize the edge image by using Otsu's threshold[4] value.

4. Gap filling process

Gap filling process is made by morphological dialation method. The value of the output pixel is the *maximum* value of all pixels in the neighborhood. In a binary image, a pixel is set to 1 if any of the neighboring pixels have the value. Morphological dilation makes objects more visible and fills in small holes in objects.

IV. RESULT AND DISCUSSION

In order to evaluate the performance of proposed method road signal scene text images are used. Here, output of text extraction results when run on are shown below.



Fig 2.Original image



Fig 3 . Output of text extraction

Precision and recall rate are used as performance measures and the proposed system compared with Wang et al[6] and Kim et al.[1].

Table 1 : Performance results of text extraction

Method / Measure	Precision rate (%)	Recall rate (%)
Proposed system	92.6	94.3
Wang et al[6]	89.8	92.1
Kim et al.[1]	63.7	82.8

In Table 1, shows precision rate and recall rate of the proposed method and that of the other existing methods. The performance of our proposed method is excellent overall. Therefore the proposed method is proved to be efficient for extracting the text from the outdoor scene images.

V . CONCLUSION

In this paper, proposed method which is presented very simple and effective algorithm for text extraction. The main aim proposed text extraction is made application easy and reducing the computation complexity. The aim is satisfied by the proposed work. According to the experimental results, the proposed method is proved to be effective and efficient for extracting the text regions from the complex scene images. There may be so many ideas for future work. But further works have to improve the efficiency of the system. So our intensions is to explore the efficincy direction in future.

REFERENCES

- [1] K.C.Kim, H.R.Byun, Y.J.Song, Y.M. Choi, S.Y.Chi, K.K. Kim and Y.K.Chung, “Scene Text Extraction in natural scene images using hierarchical feature combining and verification”, Pattern Recognition, 2004, Aug 2004, vol.2 of ICPR 2004. Proceedings of the 17 th International Conference on, pp. 679 – 682.
- [2] J. Greenhalgh and M. Mirmehdi, “Real-time detection and recognition of road traffic signs,” IEEE Transactions on Intelligent Transportation Systems, pp. 1498-1506, Dec. 2012.

- [3] Neumann et al., “Realtime Scene Text Localization and Recognition”, IEEE journal ,2012.
- [4] Otsu, N., A threshold selection method from gray-level histograms.Automatica, 1975.11(285-296): pp.23-27
- [5] H. Raj, R. Ghosh, Devanagari Text Extraction from Natural Scene Images, 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE, 2014, pp. 513-517.
- [6] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment:from error visibility to structural similarity, IEEE Trans. Image Process. 13 (2004) 600–612.
- [7] J. Zhang, R. Kasturi, A novel text detection system based on character and linkenergies, IEEE Trans. Image Process. 23 (2014) 4187–4198.

Optimizing Bigdata Processing by using Hybrid Hierarchically Distributed Data Matrix

K.L.S.Soujanya^a, B.Shirisha^b, Challa Madhavi Latha^c

^a Professor, Department of CSE, CMR College of Engineering & Technology, Hyderabad, India.

klssoujanya@cmrcet.org

^b M .Tech Student, Department of CSE, CMR College of Engineering & Technology, Hyderabad, India.

shirishabadithela@gmail.com

^c Assistant Professor, Department of Information Technology, Faculty of Informatics, University of Gondar, Gondar, Ethiopia. saidatta2009@gmail.com (Corresponding Author)

Optimizing Bigdata Processing by using Hybrid Hierarchically Distributed Data Matrix

Abstract - Data is the most valuable entity in today's world which has to be managed. The huge data available is to be processed for knowledge and predictions. This huge data in other words big data is available from various sources like Facebook, twitter and many more resources. The processing time taken by the frameworks such as Spark, MapReduce Hierarchical Distributed Matrix (HHDM) is more. Hence Hybrid Hierarchically Distributed Data Matrix (HHHDM) is proposed. This framework is used to develop Bigdata applications. In existing system developed programs are by default or automatically roughly defined, jobs are without any functionality being described to be reusable. It also reduces the ability to optimize data flow of job sequences and pipelines. To overcome the problems of existing framework we introduce a HHHDM method for developing the big data processing jobs. The proposed method is a Hybrid method which has the advantages of Hierarchical Distributed Matrix (HHDM) which is functional, strongly typed for writing big data applications which are composable. To improve the performance of executing HHHDM jobs multiple optimizations are applied to the HHHDM method. The experimental results show that the improvement of the processing time is 65-70 percent when compared to the existing technology that is spark.

Keywords: Big data processing, Optimization, Hybrid Hierarchically Distributed Data Matrix framework, strongly-typed.

I. Introduction

The exponential growth and availability of data is described by the Big data. It has become a buzz word in software environment. But the growing large-scale data is exponential as year by year recent research report says in the year of 2020 exponential growth of large-scale data is zetta bytes and yotta byte of storage in systems. For this kind of problems introduces the new development of novel solutions to overcome this problems or challenges. In general the mapreduce framework fundamental principle are move to analysis of the data, rather than moving the data to a system that (mapreduce) can analyze it.

Programmers are inviting to think in a data centric fashion by using it. Here programmers can focus on applying transformations to sets of records of data. The details of this data records are transparently managed or maintained by the framework. Framework is transparently manage the details of data records are distributed execution and fault tolerance. However, in running years in the data analytics domain

applications requirements are increasing with day to day life of software environment Hadoop framework various limitations have been recognized and we constituted a new wave of mostly domain specific , in optimized big data processing platforms with witnessed an unprecedented interest to tackle these challenges with new solutions.

In recent years with using the distributed clusters of commodity machines, more methods were presented to take care of the ever increasing data sets. Several frameworks (eg: spark)developing of big data programs and application complexity can significantly reduced by these frameworks.

The main challenges of present in big data analytical applications are listed below :

- Real time software applications and programs requires a chain of operations for processing.
- Manual optimizations are time-consuming and prone to errors. Merging, developing and interaction in big data programs is not natively supported.
- MapReduce and Spark are roughly defined and without giving any information about the functionalities. Because of this aspect the application is not reusable.

To overcome the above challenges, we a new framework HHHDM is proposed.

II. Literature Survey

Various approaches have been used for securing and maintaining the efficiency and performance of millions of data set with variety, velocity, and volume (Anju & Shyma, 2018). In the recent past, the flow of data produced by various computations has been increased and it is shifting to large scale data mechanisms. MapReduce data processing is one of the best widespread method to manage big data and it is useful for reduce processing time and memory space and also efficient parallel processing to produce large data sets (Triguero et al., 2015). Qian et al., (2015) implemented MapReduce by using an algorithm i.e. hierarchical attribute reduction. Manogaran et al., (2017) followed the same process to monitor the smart health care in a secured way. Majority of researchers has been found that the performance of data has been improved for their proposed frameworks and methods implemented by using MapReduce data processing model. However, the MapReduce framework implementations had some limitations, which are handled by some researchers. Matthew et al., (2018) overcomes the big data complications and limitations such as data storage, partitioning, transformation, retrievals, extractions, indexing etc., by generating training data set.

In intelligent transportation systems (ITS), the big data is playing major role around the globe. ITS big data is having major impacts on applications and designs of ITS, which makes the system secure and efficient (Li et al., 2018).

However, in running years in the data analytics domain applications requirements are increasing with day to day life of software environment Hadoop framework various limitations have been recognized and established a new trend of domain specific, which is a witnessed to optimize big data processing and also handle unparalleled problems with new elucidations (Sharif et al., 2013). The big data has converted to a widespread term in software environment, but the growing large-scale data is exponential as year by year recent research report says in the year of 2020 exponential growth of large-scale data is zetta bytes and yotta byte of storage in systems. Therefore, the storage related and dataset problems could be solved and overcome by using novel approaches (Sharif & Mohammad, 2014). Some researchers suggested hybrid models to solve various data set issues. The hybrid models are integrated with more than one model, which is very efficient to improve the performance, handle problems and weakness of data sets (Mohamad et al., 2016; Paradarami et al., 2017).

III. Proposed System

In order to overcome the challenges and also improve the efficiency of big data processing we propose HHHDM by integrating Map reduce with HHDM.

A. Introduction to HHDM :-

- HHDM is functional cores attribute to develop the optimization and parallel execution of big data program and applications.
- HHDM is defined as $HHDM[T,R]$. It is function in that T is input type of type T and R is output
- A part from this core objects HHDM includes data dependence, location, functionality and state.
- HHDM is strongly data type and light weight and functional defined.

B. Representation of HHDM :-

Attributes of HHDM :

1. ID : This id is identifier to the HHDM. This is must be a unique within each HHDM context.
2. INTYPE and OUTTYPE : Those are used to type correctness in programming planning and execution.
3. CATEGORY : Which category of HHDM either DDM or DFM for program execution.

4. CHILDERN and DEPENDENCY : This attributes are used to reordering the jobs or reusing the jobs of big data.
5. LOCATION : HHDM holdes the address of program (URL) it is used in any where with in the HHDM location.
6. FUNCTION: It is core attribute in HHDM it is used to how to compute the output to the programs.
7. STATE: It provides the status of the program and application

This attributes are using based on programmer design methods. By using this attributes HHDM defined of

- Functional
- Portable
- Location

Categories of HHDM :

HHDM is independent core object and tree based structure which consists of the following two types of nodes :

DDM Distributed Data Matrix:- leaf nodes of the HHDM hierarchically hold the data of all node and it is atomic operation if includes ID, SIZE, LOCATION of data jobs. It is used to path specification in HHDM defined as $HHDM[path, T]$

DFM Distributed Functional Matrix:-It is high level programming in HHDM and non leaf node hold the chilled data. It is used to composable output to the program this output is input to other subsquents. If it is in execution state it wappered the children node data and other nodes data.

Data Dependencies of HHDM:

This is further divided into four types

1. One -To- One(1:1)
2. One-To-N(1:N)
3. N-To-One(N:1)
4. N-To-N(N:N)

Advantages of proposed system:

- HHDM is a functional defined.
- Strongly-typed data type.
- It provides the reusability of jobs in programming and applications.
- Location path is available in HHDM.

IV. Implementation

HHDM Function:- is the function used for transformation of input data to out put by using various semantics. Functions have different semantics targeting different execution context for different datasets in HHDM. One HHDM function has three semantics, those are Fp, Fa, Fc :

Fp is the basic semantics of a function

$Fp : List[T] \rightarrow List[R]$

Fa is the aggregation semantics of a function

$Fa : (List[T], List[R]) \rightarrow List[R]$

Fc is the combination semantics of a function

$Fc : (List[R], List[R]) \rightarrow List[R]$

HHDM Composition:- HHDM inherits the idea of functional composition to support two basic type of composition:

$HDM[T, R] \text{ compose } HDM[I, T] \Rightarrow HDM[I, R]$

$HDM[T, R] \text{ andThen } HDM[R, U] \Rightarrow HDM[T, U]$

These two patterns are commonly used in functional programming and can be recursively used in HHDM sequences to achieve complicated composition requirements.

Interaction with HHDM : To interaction with HHDM we use five types of Actions for integration Compute, Sample, Count, Traverse, Trace. HHDM applications are designed to be interactive during runtime in an a synchronous manner

Creating a frame:-

Method:

In the first method we will be creating frame by extending Frame class which is defined in java.awt package.

In the program we are using three methods:

setTitle: For setting the title of the frame we will use this method. It takes String as an argument which will be the title name.

setVisible: For making our frame visible we will use this method. This method takes Boolean value as an argument. If we are passing true then window will be visible otherwise window will not be visible.

setSize: For setting the size of the window we will use this method. The first argument is width of the frame and second argument is height of the frame.

V. Case Study

As case study different data sets of text documents are taken for performing word count and sorting by using two methods that is HHDM and Spark. The running of the software is shown in the following figures.



Figure 1:Home screen

In the Figure 1 Home screen of the project is shown, where in the frame shows the provision for uploading the intended data set, execution type etc., using both HHDM and spark separately.

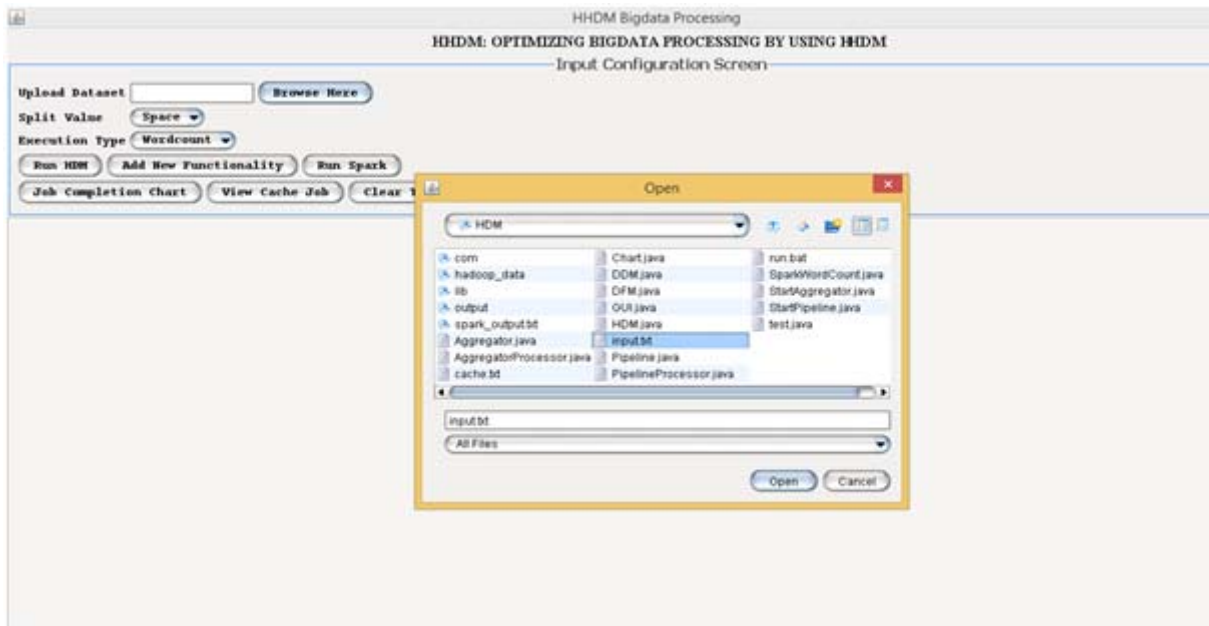


Figure 2: Upload dataset

In the Figure2 showschoosing the input file or data set from required or stored place in the system. In this step of selecting input data set we select the input data set as per our requirements and then access that input data set by using frame of open button.



Figure 3: Dataset output Type display

The Figure3 shows the information about the output display type after the execution for we have to select here the execution type frame as word count or sort. This chosen functionality will be run by HHDM on our required input.



Figure 4: Run HHDM

The Figure 4 shows the taken program execution in HHDM method. HHDM job completion time of above taken program is 1375 M.sec. In HHDM method include the DDM and DFM techniques are works as similar as MapReduce framework in Hadoop.



Figure 5: Run using Spark

The Figure 5 shows the execution of taken data set or job with spark. Then we observe the job completion time of the taken job with spark i.e., 8709M.sec

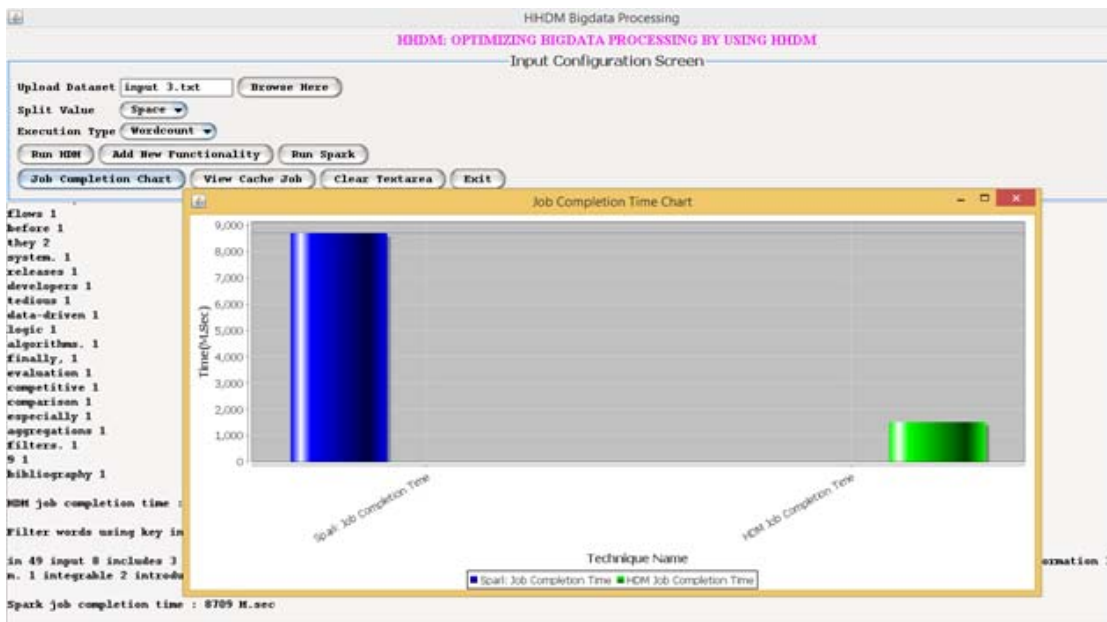


Figure 6: Job completion chart

The Figure 6 shows the result display of the job completion time for both HHDM and spark and this step of result show graph representation of the same above results. Here we observe HHDM graph length is less compare with spark i.e., HHDM job completion time is less compared with the spark job completion time.

VI. Results

The results of the execution time of the job are shown in the following Table.

Table 1: Execution time for Word Count

Input	HHDM	Spark
Test1.txt	1066	7870
Test2.txt	1078	8063
Test3.txt	1328	7907

The Table 1 shows the different job completion time of different data sets in the word count application .

For these values we have graphical representation as shown in Figure 7

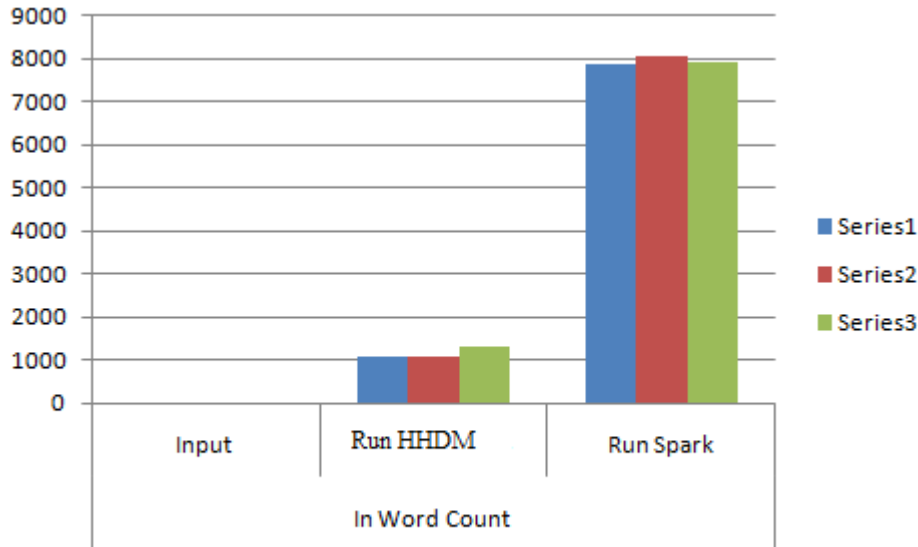


Figure :7 Graphical representation of word count jobs

In the Figure 7 the Graphical representation of word count shows that the execution time for HHDM is far less when compared to the Spark, in all the Three data sets which is represented with different colors like blue,red and green.

Table 2: Execution time for sorting.

Input	Run HHDM	Run Spark
Text1.txt	1066	7870
Text2.txt	1078	8063
Text3.txt	1328	7907

The Table 2 shows the shows the different job completion time of different data sets in the sorting technique . For these values we have graphical representation as shown in Figure 8.

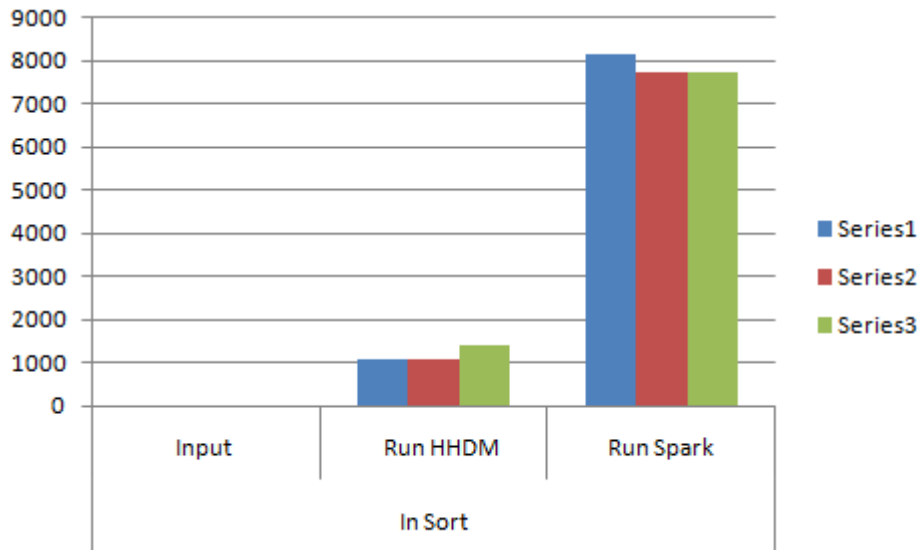


Figure : 8 Graphical representation of Sorting jobs

In the Figure 8 the Graphical representation of sorting jobs chart shows that the execution time for HHDM is far less when compared to the Spark, in all the Three data sets which is represented with different colors like blue, red and green.

VII. Conclusion

In this paper, HHDM which is a functional and strongly-typed meta-data abstraction, is implemented. Also a runtime implementation of the system to support the execution, management and optimization of HHDM applications is implemented. The applications written in HHDM are natively composable and can be merged with already existing software application. The movement of data in HHDM jobs is naturally optimized even before execution at runtime. HHDM facilitates the programmer to concentrate on the logic by automating the integration process and optimization process. The results show that the execution time is optimized when HHDM is used when compared with spark. The improvement in the performance is 65-70%.

References:

- [1] Alexander Alexandrov, Rico Bergmann, Stephan Ewen, Johann-Christoph Freytag, Fabian Hueske, Arvid Heise, Odej Kao, MarcusLeich, Ulf Leser, Volker Markl, Felix Naumann, Mathias Peters,Astrid Rheinl'ander, Matthias J. Sax, Sebastian Schelter, MareikeH'oger, Kostas Tzoumas, and Daniel Warneke." The Stratosphere Platform for Big Data analytics". VLDB J., 23(6), 2014.
- [2] Anju Abraham, and Shyma Kareem., 2018,"Security and Clustering Of Big Data in Map Reduce Framework "International Journal of Advance Research, Ideas And Innovations In Technology Volume 4, Issue 1,pp-199, ISSN:2454-132X.
- [3] Bikas Saha, Hitesh Shah, Siddharth Seth, Gopal Vijayaraghavan, Arun C Murthy, and Carlo Curino. Apache Tez:" A UnifyingFramework for Modeling and Building Data Processing Applications" .In SIGMOD, 2015.
- [4] ChunWei Tsai, Chin Feng Lai, Han Chieh Chao, and Athanasios V.Vasilakos." Big Data Analytics": a survey. Journal of Big Data, 2(21),2015.
- [5] Corrigan, P. Zikopoulos, K. Parasuraman, T. Deutsch, D. Deroos, and J. Giles," Harness the Power of Big Data the IBM Big Data Platform". 1st ed. New York, NY, USA:McGraw-Hill, Nov. 2012.
- [6] D. Sculley, Gary Holt, Daniel Golovin, Eugene Davydov, ToddPhillips, Dietmar Ebner, Vinay Chaudhary, and Michael Young.Machine learning:" The high interest credit card of Technical Debt".In SE4ML: Software Engineering for Machine Learning, 2014.
- [7] Dongyao Wu, Sherif Sakr, Liming Zhu, and Qinghua Lu." Composable and Efficient Functional Big Data Processing Framework" .In IEEE Big Data, 2015.
- [8] Jiawei Yuan, and Yifan Tian. "Practical Privacy-Preserving MapReduce Based K-means Clustering over Large-scale Dataset". IEEE, 2017.
- [9] Li Zhu, Fei Richard Yu, Yige Wang, Bin Ning and Tao Tang."Big Data Analytics in Intelligent Transportation Systems" A Survey 1524-9050 IEEE, 2018.
- [10] Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P.M., Sundarasekar, R., Thota, C.,2017. A new architecture of Internet of Things and big data ecosystem forsecured smart healthcare monitoring and alerting system. Future Gener.Comput. Syst. 82, 375–387.
- [11] Mattew Malensek, Walid Budgaga, Ryan Stern, Sangmi Lee Pallickara and Shrideep Pallickara." Trident: Distributed Storage, Analysis, and Exploration of Multidimensional Phenomena"IEEE, 2018.
- [12] Michael Armbrust, Reynold S. Xin, Cheng Lian, Yin Huai, DaviesLiu, Joseph K. Bradley, Xiangrui Meng, Tomer Kaftan, Michael J.Franklin, Ali Ghodsi, and Matei Zaharia. "Spark SQL: RelationalData Processing in Spark". In SIGMOD, pages 1383–1394, 2015.

- [13] Mohamad, M., Selamat, A., 2016. A new hybrid rough set and soft set parameter reduction method for spam e-mail classification task. *Lecture Notes in Artificial Intelligence, LNAI 9806 (9806)*, 18–30.
- [14] Paradarami, N.D., Tulasi, K., Bastian, Wightman, J.L., 2017. A hybrid recommender system using artificial neural networks. *Expert Syst. Appl.* 83, 300–313.
- [15] Qian, J., Lv, P., Yue, X., Liu, C., Jing, Z., 2015. Hierarchical attribute reduction algorithms for big data using MapReduce. *Knowl.-Based Syst.* 73, 18–31.
- [16] Sherif Sakr and Mohamed Medhat Gaber, editors. “Large Scale and Big Data - Processing and Management”. Auerbach Publications, 2014.
- [17] Sherif Sakr, Anna Liu, and Ayman G. Fayoumi. “The Family of MapReduce and Large-scale Data Processing Systems”. *ACM CSUR*, 46(1):11, 2013.
- [18] Triguero, I., Peralta, D., Bacardit, J., García, S., Herrera, F., 2015. MRPR: a MapReduce solution for prototype reduction in big data classification. *Neurocomputing* 150, 331–345.
- [19] Y. Zhang, S. Chen, Q. Wang, and G. Yu, “i2mapreduce: Incremental MapReduce for mining evolving Big Data,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, 2015.
- [20] Zhipeng Gao, Kun Niu, Yidan Fan, and Zhenyiying. “MR-Mafia: Parallel Subspace Clustering Algorithm Based on MapReduce For large Multi-dimensional Datasets” *International Conference on Big Data IEEE*, 2018.

Design and Analysis of M-Shape Microstrip Patch Antenna for Wireless Communications

Muhammad Afsar Uddin

Department of Computer Science & Engineering
Z.H. Sikder University of Science & Technology
Shariatpur, Bangladesh
afsarcste@gmail.com

Fatama Akter

Department of Computer Science & Engineering
Z.H. Sikder University of Science & Technology
Shariatpur, Bangladesh
fatama.nstu@gmail.com

Md. Zahid Hossain

Assistant Maintenance Engineer (Hardware)
Dhaka WASA
Dhaka, Bangladesh
shakil.blink@gmail.com

Abstract— The outgrowth of transportable wireless communication devices has pushed designers to design miniature size antennas. The most prized among miniature antenna selections is that the microstrip patch antenna. In this paper, A wideband M-shaped microstrip patch antenna has been designed for wireless communications such as Radar, Satellite and Microwave communications etc. A substrate of low dielectric constant named Rogers RT5880 is selected to obtain a compact radiating structure that meets the demanding bandwidth specification. The designed antenna has a dimension of 28.9mm by 24.20mm. The reflection coefficient at the input of the optimized M-shaped microstrip patch antenna is below -10 dB. The measurement results are in excellent agreement with the Sonnet Suite simulation results to analyze the performance. Simulation results show that the impedance bandwidth is 48.78% of the center frequency. This Method of Moment based simulation software provides the results in terms of S11 parameter, Return Loss, VSWR, etc. which is quite useful to analyze the antenna performance. The proposed microstrip patch antenna is suitable for C-band communication. The Bandwidth obtained for C-band communications is greater than other existing M-shape microstrip patch antennas.

Keywords- Microstrip Patch Antenna, M-shaped Patch, Substrate Thickness, Return Loss, C-band, Bandwidth, Sonnet Software.

I. INTRODUCTION

With the advancement in wireless communication technology, the necessity for lightweight and miniature size antennas [1] has become a compulsory requirement in today's world. To fulfill this requirement, a microstrip patch antenna is a good alternative and has many advantages over conventional microwave antenna and therefore is widely used in many practical applications.

Patch antennas provide several benefits not usually exhibited in different antenna configurations. For instance,

they are extraordinarily low profile, light-weight, easy and cheap to construct using modern-day computer circuit board technology, compatible with short electromagnetic wave means microwave and millimeter-wave incorporated circuits [2]. With simpler construction, microstrip patch antenna consists of a dielectric substrate on one side of a patch, with a ground plane on the other side. The assembly is typically contained inside a plastic radome, that protects the antenna structure from harm. Due to its advantages, the patch antenna is a perfect candidate for applications such as pagers, missile systems, satellite communications systems, radar, microwave, space communication and wireless local area networks (WLAN) [3]. In spite of its various attractive features, the microstrip element suffers from an inherent disadvantage of narrow impedance bandwidth and low gain [4].

In this paper, designed an M-shaped microstrip patch antenna for C-band communication covering 4-8 GHz [5] primarily used for satellite communications [5] and full-time satellite TV networks or raw satellite feeds. C-band also used for long-distance radio telecommunications, some Wi-Fi devices, cordless telephones, some weather radar systems and commonly used in areas that are subject to tropical rainfall which is the absorption of radio signals by atmospheric rain, snow or ice [5] to improve bandwidth as well as to mitigate the problems.

II. DESIGN METHOD OF PATCH ANTENNA

The design procedure for the microstrip patch antenna has designed for use in the wireless local area network (WLAN) need some important factors. The elementary factors related in the design of a single patch antenna are: Selection of substrate material, Feed position & its location and Patch dimensions [8]. For the selection of substrate, the main electrical properties to think about are relative dielectric constant and loss tangent [8]. The choice of substrate material plays a

extremely significant role in patch antenna design. The substrate thickness ought to be chosen as large as possible to maximize bandwidth and efficiency [8]. The substrate thickness decreases, the effect of the conductor and dielectric losses becomes more severe, limiting the efficiency [9]. A higher dielectric constant results in smaller patch but usually reduces bandwidth leading to tighter fabrication tolerance [8]. The M-shape microstrip patch antenna has been designed with physical parameters of W (28.9 mm) x L (24.20 mm). The dielectric substrate Rogers RT5880 and the dielectric constant of this substrate are $\epsilon_r = 2.2$ are used to design this antenna. In this patch antenna, the thickness of the substrate h is 0.9144mm and resonant frequency f_0 is 4.1 GHz. Co-axial probe feeding technique also been used here because in this feeding technique, the feed may be placed at any desired location on the patch so as to match cable impedance with the antenna input impedance [6]. For designing the patch, the width and length of the M-shape microstrip antenna are calculated as follows [7].

Width Calculation (W):

$$W = \frac{c}{2f_0 \sqrt{\frac{(\epsilon_r + 1)}{2}}} \quad (1)$$

Where C is the free-space velocity of light, ϵ_r is the dielectric constant of the substrate, f_0 is the antenna operating or resonant frequency, W is the patch non resonant width, and the effective dielectric constant is ϵ_{reff} given as

Calculation of Effective dielectric constant (ϵ_{reff}):

$$\epsilon_{reff} = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2} \left[1 + 12 \frac{h}{W} \right]^{-\frac{1}{2}} \quad (2)$$

Where h is the height of dielectric substrate and the dimensions of the microstrip patch on its length are extended on every end by a distance ΔL , that may be a function of the effective dielectric constant and also the width-to-height ratio (W/h), and the normalized extension of the length, is

Calculation of the Effective length (L_{eff}):

$$L_{eff} = \frac{c}{2f_0 \sqrt{\epsilon_{reff}}} \quad (3)$$

Calculation of the length extension (ΔL):

$$\Delta L = 0.412h \frac{(\epsilon_{reff} + 0.3) \left(\frac{W}{h} + 0.264 \right)}{(\epsilon_{reff} - 0.258) \left(\frac{W}{h} + 0.8 \right)} \quad (4)$$

Calculation of actual length of patch (L):

The actual length of the patch can be determine as

$$L_{eff} = L + 2\Delta L \quad (5)$$

III. M-SHAPE PATCH ANTENNA GEOMETRY

The M-shaped microstrip patch antenna is simpler in construction. Patch antenna is designed and simulated by using Sonnet Software which is a planar 3D electromagnetic simulator. In this antenna, feeding has been done at the purpose wherever the return loss is minimum. The method requires outstandingly precise computation of the impedance matrix but is capable of accurately predicting currents, impedance, and resonant frequency of the antenna [10]. The geometry of M-shape microstrip patch antenna with box wall port which is the most common types of port that use reference plane to remove the effects of the transmission line effect as shown in Fig. 1.

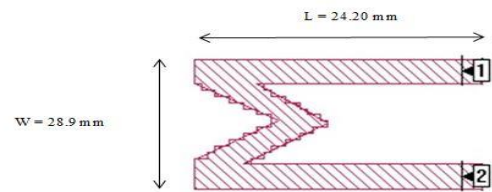


Figure 1. Top view of the M-shaped antenna

And the 3-Dimensional observation of M-shape patch antenna is shown in Fig. 2.

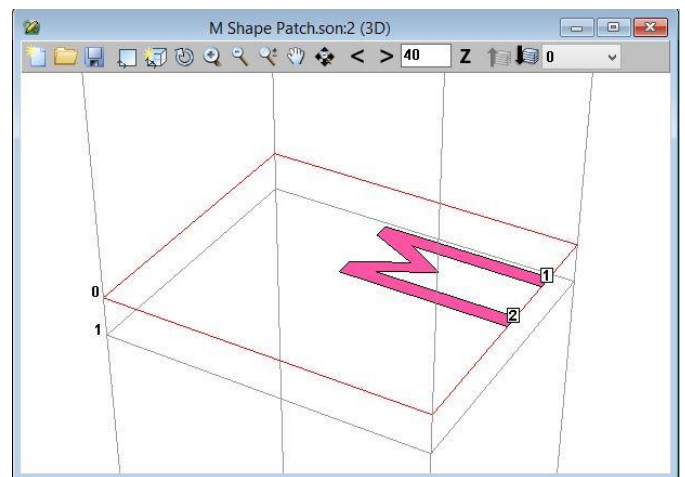


Figure 2. 3D view of the M-shape antenna

The proposed M-shape microstrip patch antenna design parameters are Dielectric material, Dielectric constant of the material, Loss tangent, Height of substrate, Width of the patch, Length of the patch and Frequency of operation is presented in Table I.

TABLE I. PROPOSED M-SHAPE PATCH ANTENNA DESIGN PARAMETERS

Antenna Design Parameter	Material / value
Dielectric Material	Rogers RT5880
Dielectric Constant(ϵ_r)	2.2
Loss Tangent	9.0e-4
Height of Substrate (Thickness) (h) (mm)	0.9144
Width of the Patch (W) (mm)	28.9
Length of the Patch (L) (mm)	24.20
Resonant Frequency (f_0) (GHz)	4.1

IV. ANTENNA SIMULATION RESULTS

In this paper, broad banding technique M-shape patch is presented. The simulation results are shown and explained below in terms of the return loss and input impedance curve. The current density on the antenna is additionally showed.

A. Return Loss Curve

The first necessary parameter is return loss curve that could be a logarithmic ratio measured in decibel that compares the ability reflected by the antenna to the power that is fed into the antenna from the transmission line [11].

The return loss curve is very much helpful to calculate the bandwidth of the antenna structure is its S11 parameter in decibel versus frequency. The return loss curve of the designed antenna is indicated in Fig. 3, and minimum S11 level of -30.89 dB is shown in m3 caption. The figure shows that the antenna resonates at 4.1GHz band.

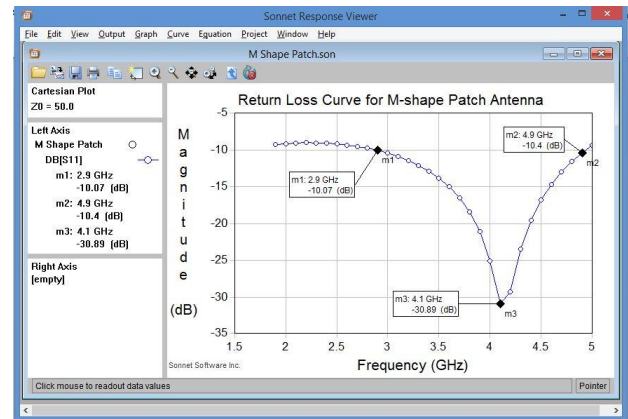


Figure 3. Simulated Return Loss Curve of M-shape patch antenna

Calculation of the bandwidth

The bandwidth can be delineated in terms of percent of the middle frequency of the band.

$$BW = \frac{F_H - F_L}{F_C} \times 100 \quad [10] \quad (6)$$

Where F_H = Higher Frequency, F_L = Lower Frequency and F_C = Center Frequency. Here $F_L = m1 = 2.9$ GHz, $F_H = m2 = 4.9$ GHz and $F_C = m3 = 4.1$ GHz. So the obtained bandwidth is 2 GHz, which is nearly 48.78% of the center frequency.

B. Input Impedance Curve

The input impedance curve gives the magnitude, phase angle and Voltage Standing Wave Ratio (VSWR) of the input impedance of the patch antenna at the respective frequencies. VSWR determines whether the required bandwidth is acceptable or not in any frequency range [12]. The Input impedance figure is shown in Fig. 4.

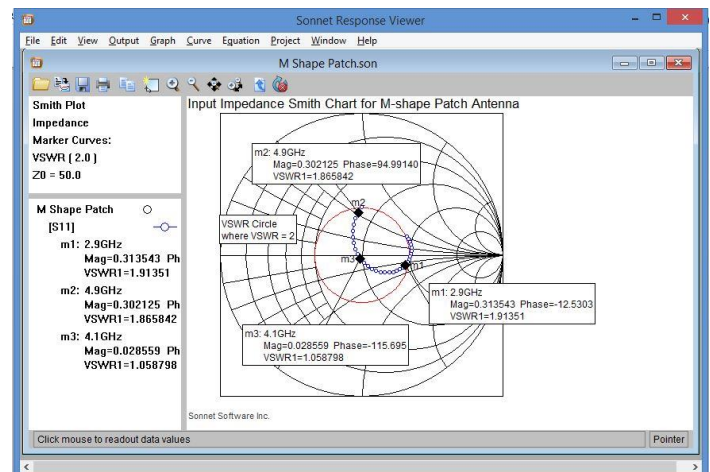


Figure 4. Input impedance curve of M-shape patch antenna

This graph shows the input impedance curve on a Smith Chart. The red circle is a VSWR curve showing VSWR = 2. From the curve it is clear that VSWR satisfies the frequency range for which bandwidth is calculated.

C. Current Density Diagram

Physical meaning of current density distribution is that it is a measure however the antenna is producing a beam. Fig. 5 is a diagram showing the current density distribution on the patch surface.

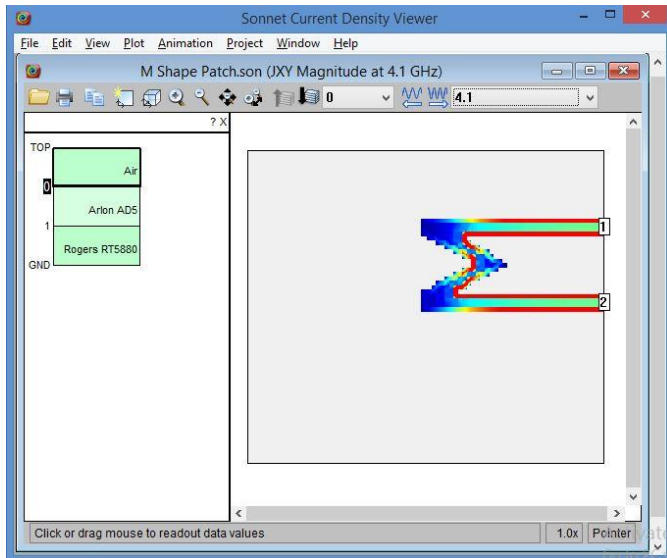


Figure 5. Current density diagram of the M-shape patch antenna at 4.1GHz

V. DISCUSSION

The bandwidth will increase because the substrate thickness increases. Here, Thickness of proposed M-shaped patch antenna is lower but obtained bandwidth is higher. Then, the substrate thickness decreases, the effect of the conductor and dielectric losses becomes more severe, limiting the efficiency. For a substrate with a moderate relative permittivity such as $\epsilon_r = 2.2$, the efficiency will be maximized. In this case, dielectric constant 2.2 is used in this proposed patch antenna. As a result, efficiency is maximum and has no conductor and dielectric losses as well as surface-wave excitation. Next, Higher dielectric constant results in the small patch, but generally reduces bandwidth. In this regard, Proposed M-shaped patch antenna has lower dielectric constant results medium sized antenna with increased bandwidth. Finally, it was taken in that bandwidth and efficiency of proposed M-shape patch are enhanced that indicates it's higher than previous M-shape patch antenna.

VI. CONCLUSION

This research work aimed at improving the bandwidth of microstrip patch antenna. Based on the theoretical, simulated and analysis of the microstrip antenna, A novel design technique for medium and compact size M shaped patch antenna is presented and discussed for wireless communication specially the satellite communication covering

C-band ranges between 4-8 GHz. The thickness of the proposed patch antennas is 0.9144mm. The VSWR parameter is less than 2 within the operating frequency range and resonant frequency is found at VSWR = 1.056. Experimental results give the better response such as return loss, VSWR, smith chart & bandwidth. These parameters presented that the losses are minimum during the transmission. And its bandwidth is improved by using the bandwidth equation. The Bandwidth obtained for C-band communications is greater than other existing M-shaped microstrip patch antenna.

VII. FUTURE SCOPES

1. Varying the feed elements to optimize the patch antenna more.
2. The efficiency of the antenna needs more analysis and a few improvements also.

REFERENCES

- [1] Sanjeev Sharma, Bharat Bhushan, Shailender Gupta and Preet Kaur, "Performance Comparison of Micro-strip Antennas with Different Shape of the Patch," International Journal of u- and e- Service, Science and Technology, Vol. 6, No. 3, pp. 13-22, June, 2013.
- [2] Arny Adila Salwa Ali and Sharlene Thiagarajah, "A Review on MIMO Antennas Employing Diversity Techniques," Proceedings of the International Conference on Electrical Engineering and Informatics Institute Technology Bandung, Indonesia, June 17-19, 2007.
- [3] Indrasen Singh, Dr. V.S. Tripathi, "Micro strip Patch Antenna and its Applications: a Survey," International Journal of Computer Technology and Applications, Vol 2(5), pp.1597-1598, 2001.
- [4] Santosh Tyagi, Kirti Vyas, "Bandwidth Enhancement Using Slotted U-Shape Microstrip Antenna with Pbg Ground," International Journal of Advanced Technology & Engineering Research, Volume 3, Issue 1, 2013.
- [5] Muhammad Afsar Uddin, Fatama Akter, Md. Jahangir Alam, "High Bandwidth F-Shaped Microstrip Patch Antenna for C-band Communications," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 3, March 2017.
- [6] Anushi Arora, Aditya Khemchandani, Yash Rawat, Shashank Singhai, Gaurav Chaitanya, "Comparative study of different Feeding Techniques for Rectangular Microstrip Patch Antenna," International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering, Vol. 3, Issue 5, May 2015.
- [7] Md. Zahid Hossain, Muhammad Afsar Uddin, Mohammed Humayan Kabir, "Bandwidth Enhancement of U-Shape Microstrip Patch Antenna," International Journal of Computer Science and Information Security, Vol.-16, No. 12, pp. 118-122, 2018.
- [8] James J. R. and Hall P. S., Handbook of microstrip antennas, Peter Peregrinus, London, UK, 1989.
- [9] M. Afsar Uddin, M. Humayan Kabir, M. Javed Hossain, and M. A. Rahman Khan, "Designing High Bandwidth Connected E-H and E-Shaped Microstrip Patch Antennas for S-band Communication," International Journal of Computer Science and Information Security, Vol. 13, No. 6, June 2015.
- [10] Edward H. Newman, Pravit Tulyathan, "Analysis of Microstrip Antenna using moment methods," IEEE Transactions on Antennas and Propagation, Vol-29(1), pp-47, 1981.
- [11] Atser A. Roy, Joseph M. Môm, Gabriel A. Igwe, "Enhancing the Bandwidth of a Microstrip Patch Antenna using Slots Shaped Patch," American Journal of Engineering Research, Volume-02, Issue-09, pp-23-30.
- [12] R. K. Prasad, Amit Kumar Gupta, Dr. D. K. Srivastava, Dr. J. P. Saini, "Design And Analysis Of Dual Frequency Band E-Shaped Microstrip

Patch Antenna,” Conference on Advances in Communication and Control Systems, 2013 (CAC2S 2013).

AUTHORS PROFILE

Muhammad Afsar Uddin is Currently serving as an Lecturer in the department of Computer Science & Engineering, Z.H. Sikder University of Science & Technology, Shariatpur, Bangladesh. He was a lecturer in the department of Computer Science & Engineering, University Of Development Alternative, Dhaka, Bangladesh. He received his B.Sc.(Engg.) degree in Computer Science & Telecommunication Engineering and M.Sc.(Engg.) degree in Telecommunication Engineering from the department of Computer Science and Telecommunication Engineering of Noakhali Science and Technology University, Noakhali, Bangladesh. His research interest includes Microstrip Patch Antenna, Network Security, Neural Networks, Data Mining and Communication Protocol.

Fatama Akter is currently pursuing as a Lecturer in the department of Computer Science & Engineering, Z.H. Sikder

Science & Technology University, Shariatpur, Bangladesh. She received her B.Sc.(Engg.) degree in Computer Science and Telecommunication Engineering from the department of Computer Science and Telecommunication Engineering of Noakhali Science and Technology University, Noakhali, Bangladesh. Her involved researches are Patch Antenna, Database Security and Big Data.

Md. Zahid Hossain is Currently serving as an Assistant Maintenance Engineer(Hardware), Dhaka WASA, Bangladesh. He received his B.Sc.(Engg.) degree in Computer Science & Telecommunication Engineering and M.Sc.(Engg.) degree in Telecommunication Engineering from the department of Computer Science and Telecommunication Engineering of Noakhali Science and Technology University, Noakhali, Bangladesh. His research topics are Microstrip Patch Antenna, Ad Hoc Network and Big Data.

Children Cognitive Load Analysis in Affordance-based Interaction

Syed Asim Ali

Department of Computer Science / UBIT, University of Karachi, Karachi -74400, Pakistan
Email: asim@uok.edu.pk

Areeba Hafeez

Institute of Business Administration, Computer Science, Karachi-74400, Pakistan
Email: sareeba22@yahoo.com

Shereen Akram

Institute of Business Administration, Computer Science, Karachi -74400, Pakistan
Email: shereenakram@live.com

Muhammad Affan Khan

Institute of Business Administration, Computer Science, Karachi -74400, Pakistan
Email: muhammadaffan.khan@khi.iba.edu.pk

Afshan Ejaz

Institute of Business Administration, Computer Science, Karachi -74400, Pakistan
Email: aejaz@iba.edu.pk

Abstract — In human-computer interaction, there are a number of design factors that designers keep in mind while designing the user interfaces to make user experiences easy and less painful. Affordance is one of that and it plays a critical role in this experience. These are the self-explanatory signs that offer the user how an object or a system can be utilized without making any efforts. In this research paper, we focused and experimentally examined how affordance-based interactions can affect the cognitive load of children's memory. We provided the children whose ages were between 7 to 12 years with the simple task to identify the positions of different objects using a mental education brain game after distracting them with a short movie clip and observed the findings which we will discuss in detail later.

Index Terms—Cognitive Load, Affordance, Working Memory, Human-Computer, Interactions

Affordance helps us perform interface based interactions more intuitively without making any effort. Psychologist J. J. Gibson (1979) proposed the concept of affordance as the available actions an object provides. He used the chair as an example to elaborate this idea that a user can afford sitting on a chair by just looking at the flat horizontal surface. According to him, the properties of a chair afford sitting on it. Later, Norman further explained that affordances are the result of our mental perception, how we see things. He further divides the term into two types. Real and perceived affordances. Real affordances can be matched with Gibson's idea whereas the perceived affordances are the one that a person can perceive based on his previous experience. (Norman, 1999; Still & Dark, 2008)

In order to get an understanding of these types, consider an example of a button named "submit" with no markup at all. It would be harder to say that it is a button. But if the same button appears at the end of a web form, we still need a little bit of processing to properly perceive it as a button. But it will be easier to

I. INTRODUCTION AND BACKGROUND

do so if the button has the markup (styling) of a button that we use in the web designing today. This means that affordances do require minimal cognitive processing (Still & Dark, 2013).

On the other hand, designers try to introduce affordances in their designs whenever possible, without thinking what kind of effect it will bring to the Working Memory (WM) to the user. WM plays a vital role in understanding UI based interactions. Baddeley (2003) defines the WM as a limited storage provided to store information for a short period of time. It is further divided into two parts namely verbal and spatial. The verbal working memory (VWM) is responsible for storing verbal information and spatial working memory is responsible for processing information about the visual appearances of an object. The other main part of the WM is the central executive which controls both VWM and SWM and make use of them at the same time.

II. RELATED WORK

It is true that the topic itself is debatable. There are a number of studies that support both the arguments. Convention based interactions which were discussed in Gibsonian framework were found affected by working memory load whereas the affordance-based were not. Therefore, designers should rethink about the fact that whether to use affordance-based interaction is helpful or not. It is observed that violation of the conventions (perceived affordances) can cost more WM load on a user because of the unexpected outcome. (Still & Dark, 2010)

It is important to understand that how affordance-based interactions can affect the WM of a person. Generally, designers think that adding affordance based interactions would be helpful as they do not require any sort of cognitive processing (Maier & Fadel, 2009). However, if the user is given a simple UI based task and his performance under a WM load suffers, we can say that this is not a resource free task and some cognitive resources do required to process the task. Also, the results of the study show that affordance-based interactions should not be considered as a resource free task. It would be better if the designers consider the WM resources of a user before introducing affordance based interactions. (JOSEPH E. GRGIC, MARY L. STILL and JEREMIAH D. STILL, "Effects

of Cognitive Load on Affordance-based Interactions", 2016)

III. METHODOLOGY

The purpose of this study is to determine the impact of affordance based interactions on children working memory. It is an empirical study in which quantitative data is collected through experiment. The targeted audience are children aged between 8 to 11 years. A total of 11 children were participate in this experiment.

The experiment has comprised of four trials and a distractor that shows after each trial. It was performed on android mobile. Mental education brain game application is used to perform these tasks. DU Recorder is used for recording the timings. An animated video is used as a distractor that shows after each trail.

All the instructions were given to each participant about the complete task. For each task different objects in pairs shows at random location for 500 milliseconds. Participants were asked to recall the location and identity of each object. Spatial working memory and verbal working memory was tested through this. The coordination of information kept in SVM and VM requires the central executive.

IV. RESULTS AND ANALYSIS

After analysis, we have come up with the following results.

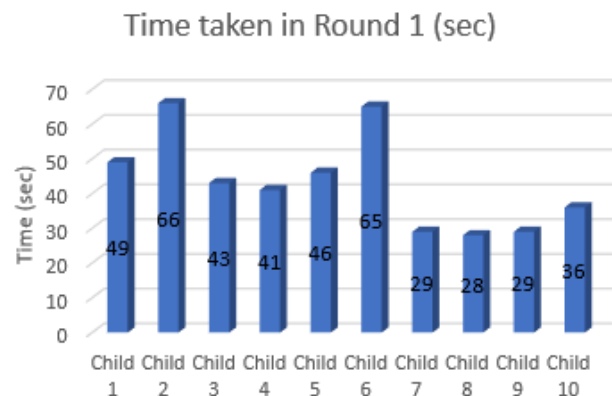


Fig 1: Time taken in first round by each participant.

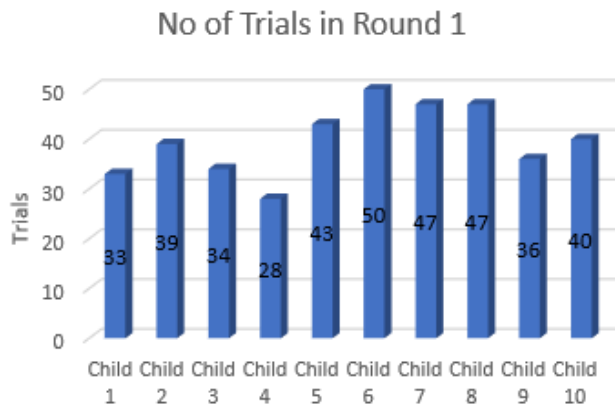


Fig 2: No of Trials in first round by each participant.

From the above graph it is derived that as for the first round most of the children are exploring and learning the game so the number of trails become more as they were learning how to play the game. Few children take much time with higher number of trails as cognitive burden increases as they have remembered each functionality of the game. Few learn them earlier as they are familiar with these types of game.

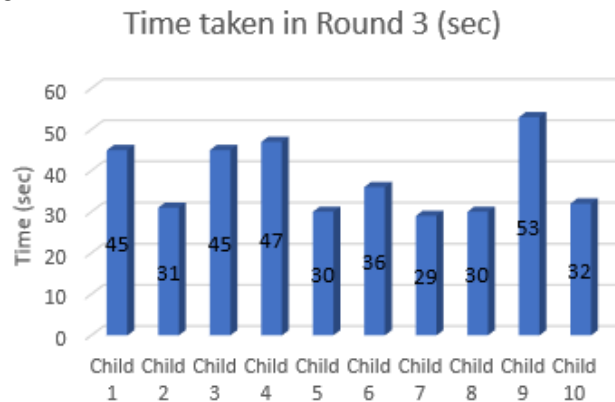


Fig 3: Time taken in third round by each participant.

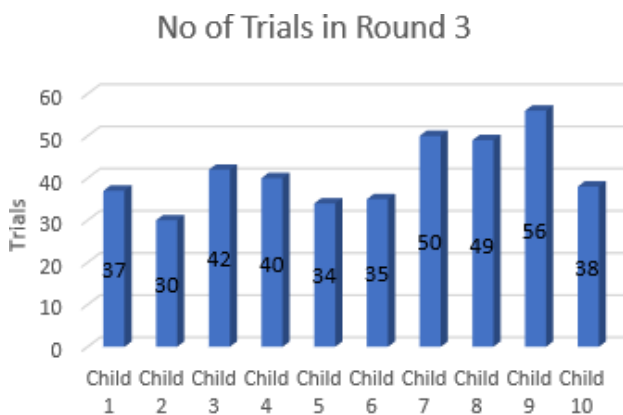


Fig 4: No of Trials in third round by each participant.

From the above graph it is derived that as the round increase the learnability of the children also improve as the familiarity with the interface also enhance as user now learn and memorize how to play the game. As good learnability impact on the number of trail, as much as user get familiar with the interface the number of trail become less. But with increase with the round the difficulty level also increases which increase the number of trails as seen in above graphs and other graph mention in Appendix A.

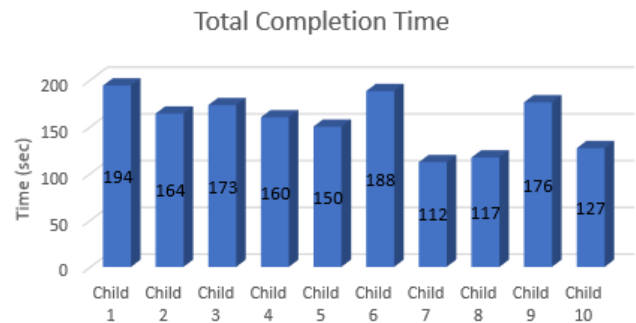


Fig 5: Completion Time (in seconds) taken by each participant.

From the above graph we can see the efficiency of the game is effect by cognitive load of the user. As the user cognitive burden increase with each level the efficiency also increase. From the above graph we can see that completion time depend upon how easily children learn to use the game as the learnability directly affect the cognitive burden of the users. Most of the users were taking time due to high recall as they have learn to remember each step.

SATISFACTION RATE

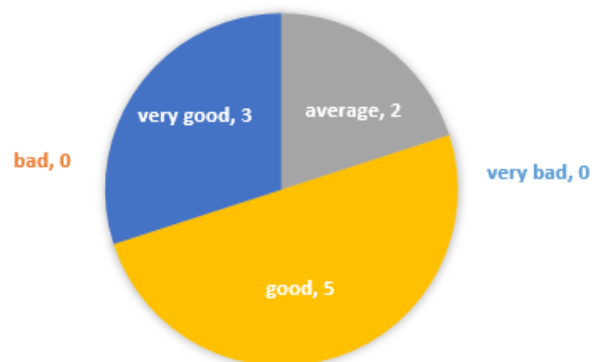


Fig 6: User Satisfaction

Results from the above figure shows the satisfaction level of participants. 50% of them rate it good.

V. CONCLUSION

From our experiment for Cognitive load analysis for Children in Affordance based interaction, we explored that Affordance based interaction do require cognitive resources. In our experiments, it is seen children uses memory resources for learnability that is directly proportional to the number of trials.

We also see from the experiment that efficiency of the game is directly proportional to cognitive load on the user. This was proven by the fact that the completion time for the game was more as users took higher time to recall each step, which in turn depends upon the cognitive load on individual player.

VI. REFERENCES

Baddeley, A. (2001). Is working memory still working? *American Psychologist*, 56, 849–864.

Nick Pettit, What Are Affordances in Web Design?, <https://blog.teamtreehouse.com/affordances-web-design>

Baddeley, A. (1992). Working memory. *Science*, 255(5044), 556–559.

J. J. Gibson (1975). 'Affordances and behavior'. In E. S. Reed & R. Jones (eds.), *Reasons for Realism: Selected Essays of James J. Gibson*, pp. 410–411. Lawrence Erlbaum, Hillsdale, NJ, 1 edn.

Norman, D. A. (1999). Affordance, conventions, and design. *Interactions*, edn 6,38–42.

JOSEPH E. GRGIC , MARY L. STILL and JEREMIAH D. STILL, “Effects of Cognitive Load on Affordance-based Interactions”, *Applied Cognitive Psychology*, Appl. Cognit. Psychol. 30: 1042–1051 (2016)

J. J. Gibson (1979). *The Ecological Approach to Visual Perception*. Houghton Mifflin Harcourt (HMH), Boston.

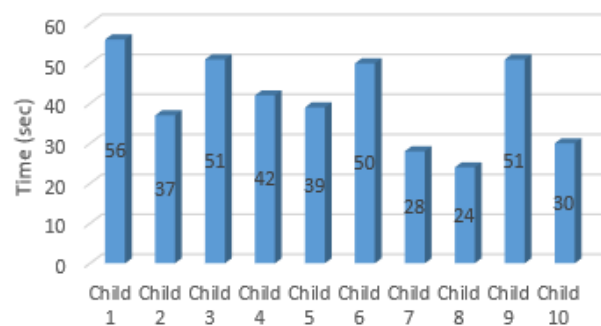
Still, J. D., & Dark, V. J. (2008). An empirical investigation of affordances and conventions. In: J. S. Gero & A. K. Goel (Eds.), *Design computing and cognition '08* (pp. 457–472). Dordrecht, The Netherlands: Springer.

Maier, J. R. A., & Fadel, G. M. (2009). Affordance based design: A relational theory for design. *Journal of Research Engineering Design*, 20, 13–27. DOI:10.1007/s00163-008-0060-3.

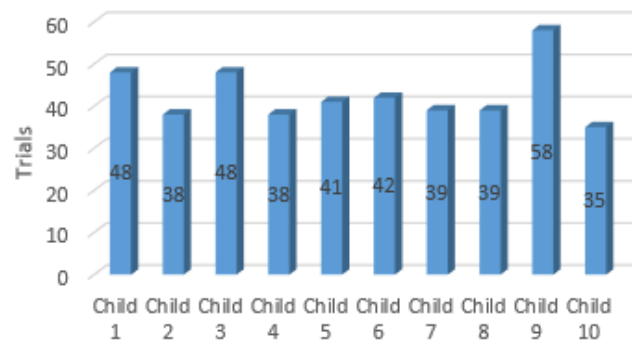
Still, J. D., & Dark, V. J. (2010). Examining working memory load and congruency effects on affordances and conventions. *International Journal Human-Computer Studies*, 68, 561–571. DOI:10.1016/j.ijhcs.2010.03.003.

VII. ANNEXURE A

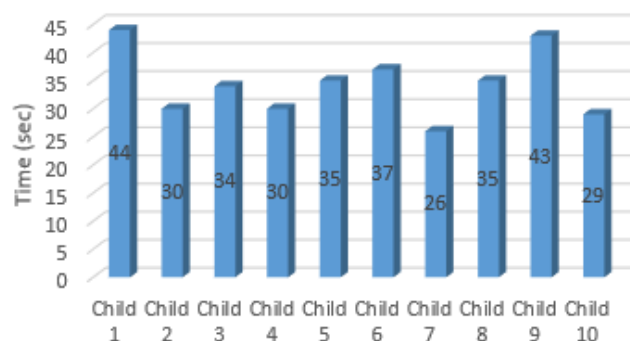
Time taken in Round 2 (sec)



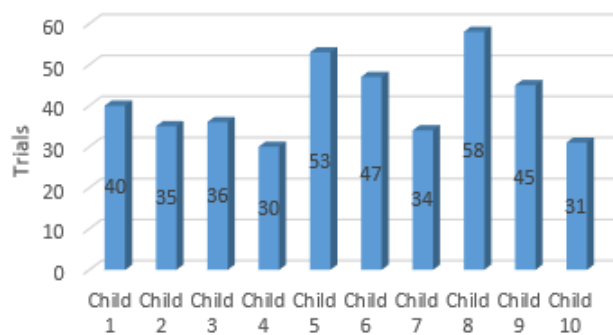
No of Trials in Round 2



Time taken in Round 4 (sec)



No of Trials in Round 4



IJCSIS REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore, Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr. Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGILIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Dr. Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr. C. Suresh Gnana Dhas, Anna University, India
Dr. Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Dr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Dr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.) / Dimat Raipur, India
Dr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Dr. A.V. Senthil Kumar, C. M. S. College of Science and Commerce, India
Dr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Dr. P. Vasant, University Technology Petronas, Malaysia
Dr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Dr. Praveen Ranjan Srivastava, BITS PILANI, India
Dr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Dr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan
Dr. Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Dr. Tirthankar Gayen, IIT Kharagpur, India
Dr. Huei-Ru Tseng, National Chiao Tung University, Taiwan
Prof. Ning Xu, Wuhan University of Technology, China
Dr. Mohammed Salem Binwahlan, Hadhramout University of Science and Technology, Yemen
& Universiti Teknologi Malaysia, Malaysia.
Dr. Aruna Ranganath, Bhoj Reddy Engineering College for Women, India
Dr. Hafeezullah Amin, Institute of Information Technology, KUST, Kohat, Pakistan

Prof. Syed S. Rizvi, University of Bridgeport, USA
Dr. Shahbaz Pervez Chattha, University of Engineering and Technology Taxila, Pakistan
Dr. Shishir Kumar, Jaypee University of Information Technology, Wakanaghat (HP), India
Dr. Shahid Mumtaz, Portugal Telecommunication, Instituto de Telecomunicações (IT) , Aveiro, Portugal
Dr. Rajesh K Shukla, Corporate Institute of Science & Technology Bhopal M P
Dr. Poonam Garg, Institute of Management Technology, India
Dr. S. Mehta, Inha University, Korea
Dr. Dilip Kumar S.M, Bangalore University, Bangalore
Prof. Malik Sikander Hayat Khiyal, Fatima Jinnah Women University, Rawalpindi, Pakistan
Dr. Virendra Gomase , Department of Bioinformatics, Padmashree Dr. D.Y. Patil University
Dr. Irraivan Elamvazuthi, University Technology PETRONAS, Malaysia
Dr. Saqib Saeed, University of Siegen, Germany
Dr. Pavan Kumar Gorakavi, IPMA-USA [YC]
Dr. Ahmed Nabih Zaki Rashed, Menoufia University, Egypt
Prof. Shishir K. Shandilya, Rukmani Devi Institute of Science & Technology, India
Dr. J. Komala Lakshmi, SNR Sons College, Computer Science, India
Dr. Muhammad Sohail, KUST, Pakistan
Dr. Manjaiah D.H, Mangalore University, India
Dr. S Santhosh Baboo, D.G.Vaishnav College, Chennai, India
Prof. Dr. Mokhtar Beldjehem, Sainte-Anne University, Halifax, NS, Canada
Dr. Deepak Laxmi Narasimha, University of Malaya, Malaysia
Prof. Dr. Arunkumar Thangavelu, Vellore Institute Of Technology, India
Dr. M. Azath, Anna University, India
Dr. Md. Rabiul Islam, Rajshahi University of Engineering & Technology (RUET), Bangladesh
Dr. Aas Alaa Zaidan Ansaef, Multimedia University, Malaysia
Dr. Suresh Jain, Devi Ahilya University, Indore (MP) India,
Dr. Mohammed M. Kadhum, Universiti Utara Malaysia
Dr. Hanumanthappa. J. University of Mysore, India
Dr. Syed Ishtiaque Ahmed, Bangladesh University of Engineering and Technology (BUET)
Dr. Akinola Solomon Olalekan, University of Ibadan, Ibadan, Nigeria
Dr. Santosh K. Pandey, The Institute of Chartered Accountants of India
Dr. P. Vasant, Power Control Optimization, Malaysia
Dr. Petr Ivankov, Automatika - S, Russian Federation
Dr. Utkarsh Seetha, Data Infosys Limited, India
Mrs. Priti Maheshwary, Maulana Azad National Institute of Technology, Bhopal
Dr. (Mrs) Padmavathi Ganapathi, Avinashilingam University for Women, Coimbatore
Assist. Prof. A. Neela madheswari, Anna university, India
Prof. Ganesan Ramachandra Rao, PSG College of Arts and Science, India
Mr. Kamanashis Biswas, Daffodil International University, Bangladesh
Dr. Atul Gonsai, Saurashtra University, Gujarat, India
Mr. Angkoon Phinyomark, Prince of Songkla University, Thailand
Mrs. G. Nalini Priya, Anna University, Chennai
Dr. P. Subashini, Avinashilingam University for Women, India
Assoc. Prof. Vijay Kumar Chakka, Dhirubhai Ambani IICT, Gandhinagar ,Gujarat
Mr. Jitendra Agrawal, : Rajiv Gandhi Proudhyogiki Vishwavidyalaya, Bhopal
Mr. Vishal Goyal, Department of Computer Science, Punjabi University, India
Dr. R. Baskaran, Department of Computer Science and Engineering, Anna University, Chennai

Assist. Prof. Kanwalvir Singh Dhindsa, B.B.S.B.Engg.College, Fatehgarh Sahib (Punjab), India
Dr. Jamal Ahmad Dargham, School of Engineering and Information Technology, Universiti Malaysia Sabah
Mr. Nitin Bhatia, DAV College, India
Dr. Dhavachelvan Ponnurangam, Pondicherry Central University, India
Dr. Mohd Faizal Abdollah, University of Technical Malaysia, Malaysia
Assist. Prof. Sonal Chawla, Panjab University, India
Dr. Abdul Wahid, AKG Engg. College, Ghaziabad, India
Mr. Arash Habibi Lashkari, University of Malaya (UM), Malaysia
Mr. Md. Rajibul Islam, Ibnu Sina Institute, University Technology Malaysia
Professor Dr. Sabu M. Thampi, .B.S Institute of Technology for Women, Kerala University, India
Mr. Noor Muhammed Nayeem, Université Lumière Lyon 2, 69007 Lyon, France
Dr. Himanshu Aggarwal, Department of Computer Engineering, Punjabi University, India
Prof R. Naidoo, Dept of Mathematics/Center for Advanced Computer Modelling, Durban University of Technology,
Durban, South Africa
Prof. Mydhili K Nair, Visweswaraiah Technological University, Bangalore, India
M. Prabu, Adhiyamaan College of Engineering/Anna University, India
Mr. Swakkhar Shatabda, United International University, Bangladesh
Dr. Abdur Rashid Khan, ICIT, Gomal University, Dera Ismail Khan, Pakistan
Mr. H. Abdul Shabeer, I-Nautix Technologies, Chennai, India
Dr. M. Aramudhan, Perunthalaivar Kamarajar Institute of Engineering and Technology, India
Dr. M. P. Thapliyal, Department of Computer Science, HNB Garhwal University (Central University), India
Dr. Shahaboddin Shamshirband, Islamic Azad University, Iran
Mr. Zeashan Hameed Khan, Université de Grenoble, France
Prof. Anil K Ahlawat, Ajay Kumar Garg Engineering College, Ghaziabad, UP Technical University, Lucknow
Mr. Longe Olumide Babatope, University Of Ibadan, Nigeria
Associate Prof. Raman Maini, University College of Engineering, Punjabi University, India
Dr. Maslin Masrom, University Technology Malaysia, Malaysia
Sudipta Chattopadhyay, Jadavpur University, Kolkata, India
Dr. Dang Tuan NGUYEN, University of Information Technology, Vietnam National University - Ho Chi Minh City
Dr. Mary Lourde R., BITS-PILANI Dubai, UAE
Dr. Abdul Aziz, University of Central Punjab, Pakistan
Mr. Karan Singh, Gautam Budtha University, India
Mr. Avinash Pokhriyal, Uttar Pradesh Technical University, Lucknow, India
Associate Prof Dr Zuraini Ismail, University Technology Malaysia, Malaysia
Assistant Prof. Yasser M. Alginahi, Taibah University, Madinah Munawwarah, KSA
Mr. Dakshina Ranjan Kisku, West Bengal University of Technology, India
Mr. Raman Kumar, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India
Associate Prof. Samir B. Patel, Institute of Technology, Nirma University, India
Dr. M. Munir Ahamed Rabbani, B. S. Abdur Rahman University, India
Asst. Prof. Koushik Majumder, West Bengal University of Technology, India
Dr. Alex Pappachen James, Queensland Micro-nanotechnology center, Griffith University, Australia
Assistant Prof. S. Hariharan, B.S. Abdur Rahman University, India
Asst Prof. Jasmine. K. S, R.V.College of Engineering, India
Mr Naushad Ali Mamode Khan, Ministry of Education and Human Resources, Mauritius
Prof. Mahesh Goyani, G H Patel Collge of Engg. & Tech, V.V.N, Anand, Gujarat, India
Dr. Mana Mohammed, University of Tlemcen, Algeria
Prof. Jatinder Singh, Universal Institution of Engg. & Tech. CHD, India

Mrs. M. Anandhavalli Gauthaman, Sikkim Manipal Institute of Technology, Majitar, East Sikkim
Dr. Bin Guo, Institute Telecom SudParis, France
Mrs. Maleika Mehr Nigar Mohamed Heenaye-Mamode Khan, University of Mauritius
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Mr. V. Bala Dhandayuthapani, Mekelle University, Ethiopia
Dr. Irfan Syamsuddin, State Polytechnic of Ujung Pandang, Indonesia
Mr. Kavi Kumar Khedo, University of Mauritius, Mauritius
Mr. Ravi Chandiran, Zagro Singapore Pte Ltd. Singapore
Mr. Milindkumar V. Sarode, Jawaharlal Darda Institute of Engineering and Technology, India
Dr. Shamimul Qamar, KSJ Institute of Engineering & Technology, India
Dr. C. Arun, Anna University, India
Assist. Prof. M.N.Birje, Basaveshwar Engineering College, India
Prof. Hamid Reza Naji, Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran
Assist. Prof. Debasis Giri, Department of Computer Science and Engineering, Haldia Institute of Technology
Subhabrata Barman, Haldia Institute of Technology, West Bengal
Mr. M. I. Lali, COMSATS Institute of Information Technology, Islamabad, Pakistan
Dr. Feroz Khan, Central Institute of Medicinal and Aromatic Plants, Lucknow, India
Mr. R. Nagendran, Institute of Technology, Coimbatore, Tamilnadu, India
Mr. Amnach Khawne, King Mongkut's Institute of Technology Ladkrabang, Ladkrabang, Bangkok, Thailand
Dr. P. Chakrabarti, Sir Padampat Singhanian University, Udaipur, India
Mr. Nafiz Imtiaz Bin Hamid, Islamic University of Technology (IUT), Bangladesh.
Shahab-A. Shamshirband, Islamic Azad University, Chalous, Iran
Prof. B. Priestly Shan, Anna Univeristy, Tamilnadu, India
Venkatramreddy Velma, Dept. of Bioinformatics, University of Mississippi Medical Center, Jackson MS USA
Akshi Kumar, Dept. of Computer Engineering, Delhi Technological University, India
Dr. Umesh Kumar Singh, Vikram University, Ujjain, India
Mr. Serguei A. Mokhov, Concordia University, Canada
Mr. Lai Khin Wee, Universiti Teknologi Malaysia, Malaysia
Dr. Awadhesh Kumar Sharma, Madan Mohan Malviya Engineering College, India
Mr. Syed R. Rizvi, Analytical Services & Materials, Inc., USA
Dr. S. Karthik, SNS College of Technology, India
Mr. Syed Qasim Bukhari, CIMET (Universidad de Granada), Spain
Mr. A.D.Potgantwar, Pune University, India
Dr. Himanshu Aggarwal, Punjabi University, India
Mr. Rajesh Ramachandran, Naipunya Institute of Management and Information Technology, India
Dr. K.L. Shunmuganathan, R.M.K Engg College , Kavaraipettai ,Chennai
Dr. Prasant Kumar Pattnaik, KIST, India.
Dr. Ch. Aswani Kumar, VIT University, India
Mr. Ijaz Ali Shoukat, King Saud University, Riyadh KSA
Mr. Arun Kumar, Sir Padam Pat Singhanian University, Udaipur, Rajasthan
Mr. Muhammad Imran Khan, Universiti Teknologi PETRONAS, Malaysia
Dr. Natarajan Meghanathan, Jackson State University, Jackson, MS, USA
Mr. Mohd Zaki Bin Mas'ud, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia
Prof. Dr. R. Geetharamani, Dept. of Computer Science and Eng., Rajalakshmi Engineering College, India
Dr. Smita Rajpal, Institute of Technology and Management, Gurgaon, India
Dr. S. Abdul Khader Jilani, University of Tabuk, Tabuk, Saudi Arabia
Mr. Syed Jamal Haider Zaidi, Bahria University, Pakistan

Dr. N. Devarajan, Government College of Technology, Coimbatore, Tamilnadu, INDIA
Mr. R. Jagadeesh Kannan, RMK Engineering College, India
Mr. Deo Prakash, Shri Mata Vaishno Devi University, India
Mr. Mohammad Abu Naser, Dept. of EEE, IUT, Gazipur, Bangladesh
Assist. Prof. Prasun Ghosal, Bengal Engineering and Science University, India
Mr. Md. Golam Kaosar, School of Engineering and Science, Victoria University, Melbourne City, Australia
Mr. R. Mahammad Shafi, Madanapalle Institute of Technology & Science, India
Dr. F. Sagayaraj Francis, Pondicherry Engineering College, India
Dr. Ajay Goel, HIET, Kaithal, India
Mr. Nayak Sunil Kashibarao, Bahirji Smarak Mahavidyalaya, India
Mr. Suhas J Manangi, Microsoft India
Dr. Kalyankar N. V., Yeshwant Mahavidyalaya, Nanded, India
Dr. K.D. Verma, S.V. College of Post graduate studies & Research, India
Dr. Amjad Rehman, University Technology Malaysia, Malaysia
Mr. Rachit Garg, L K College, Jalandhar, Punjab
Mr. J. William, M.A.M college of Engineering, Trichy, Tamilnadu, India
Prof. Jue-Sam Chou, Nanhua University, College of Science and Technology, Taiwan
Dr. Thorat S.B., Institute of Technology and Management, India
Mr. Ajay Prasad, Sir Padampat Singhanian University, Udaipur, India
Dr. Kamaljit I. Lakhtaria, Atmiya Institute of Technology & Science, India
Mr. Syed Rafiul Hussain, Ahsanullah University of Science and Technology, Bangladesh
Mrs Fazeela Tunnisa, Najran University, Kingdom of Saudi Arabia
Mrs Kavita Taneja, Maharishi Markandeshwar University, Haryana, India
Mr. Maniyar Shiraz Ahmed, Najran University, Najran, KSA
Mr. Anand Kumar, AMC Engineering College, Bangalore
Dr. Rakesh Chandra Gangwar, Beant College of Engg. & Tech., Gurdaspur (Punjab) India
Dr. V V Rama Prasad, Sree Vidyanikethan Engineering College, India
Assist. Prof. Neetesh Kumar Gupta, Technocrats Institute of Technology, Bhopal (M.P.), India
Mr. Ashish Seth, Uttar Pradesh Technical University, Lucknow, UP India
Dr. V V S S Balaram, Sreenidhi Institute of Science and Technology, India
Mr Rahul Bhatia, Lingaya's Institute of Management and Technology, India
Prof. Niranjana Reddy, P, KITS, Warangal, India
Prof. Rakesh. Lingappa, Vijetha Institute of Technology, Bangalore, India
Dr. Mohammed Ali Hussain, Nimra College of Engineering & Technology, Vijayawada, A.P., India
Dr. A. Srinivasan, MNM Jain Engineering College, Rajiv Gandhi Salai, Thorapakkam, Chennai
Mr. Rakesh Kumar, M.M. University, Mullana, Ambala, India
Dr. Lena Khaled, Zarqa Private University, Aman, Jordan
Ms. Supriya Kapoor, Patni/Lingaya's Institute of Management and Tech., India
Dr. Tossapon Boongoen, Aberystwyth University, UK
Dr. Bilal Alatas, Firat University, Turkey
Assist. Prof. Jyoti Praakash Singh, Academy of Technology, India
Dr. Ritu Soni, GNG College, India
Dr. Mahendra Kumar, Sagar Institute of Research & Technology, Bhopal, India.
Dr. Binod Kumar, Lakshmi Narayan College of Tech. (LNCT) Bhopal India
Dr. Muzhir Shaban Al-Ani, Amman Arab University Amman – Jordan
Dr. T.C. Manjunath, ATRIA Institute of Tech, India
Mr. Muhammad Zakarya, COMSATS Institute of Information Technology (CIIT), Pakistan

Assist. Prof. Harmunish Taneja, M. M. University, India
Dr. Chitra Dhawale , SICSR, Model Colony, Pune, India
Mrs Sankari Muthukaruppan, Nehru Institute of Engineering and Technology, Anna University, India
Mr. Aaqif Afzaal Abbasi, National University Of Sciences And Technology, Islamabad
Prof. Ashutosh Kumar Dubey, Trinity Institute of Technology and Research Bhopal, India
Mr. G. Appasami, Dr. Pauls Engineering College, India
Mr. M Yasin, National University of Science and Tech, karachi (NUST), Pakistan
Mr. Yaser Miaji, University Utara Malaysia, Malaysia
Mr. Shah Ahsanul Haque, International Islamic University Chittagong (IIUC), Bangladesh
Prof. (Dr) Syed Abdul Sattar, Royal Institute of Technology & Science, India
Dr. S. Sasikumar, Roever Engineering College
Assist. Prof. Monit Kapoor, Maharishi Markandeshwar University, India
Mr. Nwaocha Vivian O, National Open University of Nigeria
Dr. M. S. Vijaya, GR Govindarajulu School of Applied Computer Technology, India
Assist. Prof. Chakresh Kumar, Manav Rachna International University, India
Mr. Kunal Chadha , R&D Software Engineer, Gemalto, Singapore
Mr. Mueen Uddin, Universiti Teknologi Malaysia, UTM , Malaysia
Dr. Dhuha Basheer abdullah, Mosul university, Iraq
Mr. S. Audithan, Annamalai University, India
Prof. Vijay K Chaudhari, Technocrats Institute of Technology , India
Associate Prof. Mohd Ilyas Khan, Technocrats Institute of Technology , India
Dr. Vu Thanh Nguyen, University of Information Technology, HoChiMinh City, VietNam
Assist. Prof. Anand Sharma, MITS, Lakshmangarh, Sikar, Rajasthan, India
Prof. T V Narayana Rao, HITAM Engineering college, Hyderabad
Mr. Deepak Gour, Sir Padampat Singhania University, India
Assist. Prof. Amutharaj Joyson, Kalasalingam University, India
Mr. Ali Balador, Islamic Azad University, Iran
Mr. Mohit Jain, Maharaja Surajmal Institute of Technology, India
Mr. Dilip Kumar Sharma, GLA Institute of Technology & Management, India
Dr. Debojyoti Mitra, Sir padampat Singhania University, India
Dr. Ali Dehghantanha, Asia-Pacific University College of Technology and Innovation, Malaysia
Mr. Zhao Zhang, City University of Hong Kong, China
Prof. S.P. Setty, A.U. College of Engineering, India
Prof. Patel Rakeshkumar Kantilal, Sankalchand Patel College of Engineering, India
Mr. Biswajit Bhowmik, Bengal College of Engineering & Technology, India
Mr. Manoj Gupta, Apex Institute of Engineering & Technology, India
Assist. Prof. Ajay Sharma, Raj Kumar Goel Institute Of Technology, India
Assist. Prof. Ramveer Singh, Raj Kumar Goel Institute of Technology, India
Dr. Hanan Elazhary, Electronics Research Institute, Egypt
Dr. Hosam I. Faiq, USM, Malaysia
Prof. Dipti D. Patil, MAEER's MIT College of Engg. & Tech, Pune, India
Assist. Prof. Devendra Chack, BCT Kumaon engineering College Dwarahat Almora, India
Prof. Manpreet Singh, M. M. Engg. College, M. M. University, India
Assist. Prof. M. Sadiq ali Khan, University of Karachi, Pakistan
Mr. Prasad S. Halgaonkar, MIT - College of Engineering, Pune, India
Dr. Imran Ghani, Universiti Teknologi Malaysia, Malaysia
Prof. Varun Kumar Kakar, Kumaon Engineering College, Dwarahat, India

Assist. Prof. Nisheeth Joshi, Apaji Institute, Banasthali University, Rajasthan, India
Associate Prof. Kunwar S. Vaisla, VCT Kumaon Engineering College, India
Prof Anupam Choudhary, Bhilai School Of Engg., Bhilai (C.G.), India
Mr. Divya Prakash Shrivastava, Al Jabal Al garbi University, Zawya, Libya
Associate Prof. Dr. V. Radha, Avinashilingam Deemed university for women, Coimbatore.
Dr. Kasarapu Ramani, JNT University, Anantapur, India
Dr. Anuraag Awasthi, Jayoti Vidyapeeth Womens University, India
Dr. C G Ravichandran, R V S College of Engineering and Technology, India
Dr. Mohamed A. Deriche, King Fahd University of Petroleum and Minerals, Saudi Arabia
Mr. Abbas Karimi, Universiti Putra Malaysia, Malaysia
Mr. Amit Kumar, Jaypee University of Engg. and Tech., India
Dr. Nikolai Stoianov, Defense Institute, Bulgaria
Assist. Prof. S. Ranichandra, KSR College of Arts and Science, Tiruchencode
Mr. T.K.P. Rajagopal, Diamond Horse International Pvt Ltd, India
Dr. Md. Ekramul Hamid, Rajshahi University, Bangladesh
Mr. Hemanta Kumar Kalita, TATA Consultancy Services (TCS), India
Dr. Messaouda Azzouzi, Ziane Achour University of Djelfa, Algeria
Prof. (Dr.) Juan Jose Martinez Castillo, "Gran Mariscal de Ayacucho" University and Acantelys research Group, Venezuela
Dr. Jatinderkumar R. Saini, Narmada College of Computer Application, India
Dr. Babak Bashari Rad, University Technology of Malaysia, Malaysia
Dr. Nighat Mir, Effat University, Saudi Arabia
Prof. (Dr.) G.M.Nasira, Sasurie College of Engineering, India
Mr. Varun Mittal, Gemalto Pte Ltd, Singapore
Assist. Prof. Mrs P. Banumathi, Kathir College Of Engineering, Coimbatore
Assist. Prof. Quan Yuan, University of Wisconsin-Stevens Point, US
Dr. Pranam Paul, Narula Institute of Technology, Agarpara, West Bengal, India
Assist. Prof. J. Ramkumar, V.L.B Janakiammal college of Arts & Science, India
Mr. P. Sivakumar, Anna university, Chennai, India
Mr. Md. Humayun Kabir Biswas, King Khalid University, Kingdom of Saudi Arabia
Mr. Mayank Singh, J.P. Institute of Engg & Technology, Meerut, India
HJ. Kamaruzaman Jusoff, Universiti Putra Malaysia
Mr. Nikhil Patrick Lobo, CADES, India
Dr. Amit Wason, Rayat-Bahra Institute of Engineering & Boi-Technology, India
Dr. Rajesh Shrivastava, Govt. Benazir Science & Commerce College, Bhopal, India
Assist. Prof. Vishal Bharti, DCE, Gurgaon
Mrs. Sunita Bansal, Birla Institute of Technology & Science, India
Dr. R. Sudhakar, Dr.Mahalingam college of Engineering and Technology, India
Dr. Amit Kumar Garg, Shri Mata Vaishno Devi University, Katra(J&K), India
Assist. Prof. Raj Gaurang Tiwari, AZAD Institute of Engineering and Technology, India
Mr. Hamed Taherdoost, Tehran, Iran
Mr. Amin Daneshmand Malayeri, YRC, IAU, Malayer Branch, Iran
Mr. Shantanu Pal, University of Calcutta, India
Dr. Terry H. Walcott, E-Promag Consultancy Group, United Kingdom
Dr. Ezekiel U OKIKE, University of Ibadan, Nigeria
Mr. P. Mahalingam, Caledonian College of Engineering, Oman
Dr. Mahmoud M. A. Abd Ellatif, Mansoura University, Egypt

Prof. Kunwar S. Vaisla, BCT Kumaon Engineering College, India
Prof. Mahesh H. Panchal, Kalol Institute of Technology & Research Centre, India
Mr. Muhammad Asad, Technical University of Munich, Germany
Mr. AliReza Shams Shafigh, Azad Islamic university, Iran
Prof. S. V. Nagaraj, RMK Engineering College, India
Mr. Ashikali M Hasan, Senior Researcher, CelNet security, India
Dr. Adnan Shahid Khan, University Technology Malaysia, Malaysia
Mr. Prakash Gajanan Burade, Nagpur University/ITM college of engg, Nagpur, India
Dr. Jagdish B.Helonde, Nagpur University/ITM college of engg, Nagpur, India
Professor, Doctor BOUHORMA Mohammed, Univertsity Abdelmalek Essaadi, Morocco
Mr. K. Thirumalaivasan, Pondicherry Engg. College, India
Mr. Umbarkar Anantkumar Janardan, Walchand College of Engineering, India
Mr. Ashish Chaurasia, Gyan Ganga Institute of Technology & Sciences, India
Mr. Sunil Taneja, Kurukshetra University, India
Mr. Fauzi Adi Rafrastara, Dian Nuswantoro University, Indonesia
Dr. Yaduvir Singh, Thapar University, India
Dr. Ioannis V. Koskosas, University of Western Macedonia, Greece
Dr. Vasantha Kalyani David, Avinashilingam University for women, Coimbatore
Dr. Ahmed Mansour Manasrah, Universiti Sains Malaysia, Malaysia
Miss. Nazanin Sadat Kazazi, University Technology Malaysia, Malaysia
Mr. Saeed Rasouli Heikalabad, Islamic Azad University - Tabriz Branch, Iran
Assoc. Prof. Dharendra Mishra, SVKM's NMIMS University, India
Prof. Shapoor Zarei, UAE Inventors Association, UAE
Prof. B.Raja Sarath Kumar, Lenora College of Engineering, India
Dr. Bashir Alam, Jamia millia Islamia, Delhi, India
Prof. Anant J Umbarkar, Walchand College of Engg., India
Assist. Prof. B. Bharathi, Sathyabama University, India
Dr. Fokrul Alom Mazarbhuiya, King Khalid University, Saudi Arabia
Prof. T.S.Jeyali Laseeth, Anna University of Technology, Tirunelveli, India
Dr. M. Balraju, Jawahar Lal Nehru Technological University Hyderabad, India
Dr. Vijayalakshmi M. N., R.V.College of Engineering, Bangalore
Prof. Walid Moudani, Lebanese University, Lebanon
Dr. Saurabh Pal, VBS Purvanchal University, Jaunpur, India
Associate Prof. Suneet Chaudhary, Dehradun Institute of Technology, India
Associate Prof. Dr. Manuj Darbari, BBD University, India
Ms. Prema Selvaraj, K.S.R College of Arts and Science, India
Assist. Prof. Ms.S.Sasikala, KSR College of Arts & Science, India
Mr. Sukhvinder Singh Deora, NC Institute of Computer Sciences, India
Dr. Abhay Bansal, Amity School of Engineering & Technology, India
Ms. Sumita Mishra, Amity School of Engineering and Technology, India
Professor S. Viswanadha Raju, JNT University Hyderabad, India
Mr. Asghar Shahrzad Khashandarag, Islamic Azad University Tabriz Branch, India
Mr. Manoj Sharma, Panipat Institute of Engg. & Technology, India
Mr. Shakeel Ahmed, King Faisal University, Saudi Arabia
Dr. Mohamed Ali Mahjoub, Institute of Engineer of Monastir, Tunisia
Mr. Adri Jovin J.J., SriGuru Institute of Technology, India
Dr. Sukumar Senthilkumar, Universiti Sains Malaysia, Malaysia

Mr. Rakesh Bharati, Dehradun Institute of Technology Dehradun, India
Mr. Shervan Fekri Ershad, Shiraz International University, Iran
Mr. Md. Safiqul Islam, Daffodil International University, Bangladesh
Mr. Mahmudul Hasan, Daffodil International University, Bangladesh
Prof. Mandakini Tayade, UIT, RGTU, Bhopal, India
Ms. Sarla More, UIT, RGTU, Bhopal, India
Mr. Tushar Hrishikesh Jaware, R.C. Patel Institute of Technology, Shirpur, India
Ms. C. Divya, Dr G R Damodaran College of Science, Coimbatore, India
Mr. Fahimuddin Shaik, Annamacharya Institute of Technology & Sciences, India
Dr. M. N. Giri Prasad, JNTUCE, Pulivendula, A.P., India
Assist. Prof. Chintan M Bhatt, Charotar University of Science And Technology, India
Prof. Sahista Machchhar, Marwadi Education Foundation's Group of institutions, India
Assist. Prof. Navnish Goel, S. D. College Of Engineering & Technology, India
Mr. Khaja Kamaluddin, Sirt University, Sirt, Libya
Mr. Mohammad Zaidul Karim, Daffodil International, Bangladesh
Mr. M. Vijayakumar, KSR College of Engineering, Tiruchengode, India
Mr. S. A. Ahsan Rajon, Khulna University, Bangladesh
Dr. Muhammad Mohsin Nazir, LCW University Lahore, Pakistan
Mr. Mohammad Asadul Hoque, University of Alabama, USA
Mr. P.V.Sarathchand, Indur Institute of Engineering and Technology, India
Mr. Durgesh Samadhiya, Chung Hua University, Taiwan
Dr Venu Kuthadi, University of Johannesburg, Johannesburg, RSA
Dr. (Er) Jasvir Singh, Guru Nanak Dev University, Amritsar, Punjab, India
Mr. Jasmin Cosic, Min. of the Interior of Una-sana canton, B&H, Bosnia and Herzegovina
Dr S. Rajalakshmi, Botho College, South Africa
Dr. Mohamed Sarrab, De Montfort University, UK
Mr. Basappa B. Kodada, Canara Engineering College, India
Assist. Prof. K. Ramana, Annamacharya Institute of Technology and Sciences, India
Dr. Ashu Gupta, Apeejay Institute of Management, Jalandhar, India
Assist. Prof. Shaik Rasool, Shadan College of Engineering & Technology, India
Assist. Prof. K. Suresh, Annamacharya Institute of Tech & Sci. Rajampet, AP, India
Dr . G. Singaravel, K.S.R. College of Engineering, India
Dr B. G. Geetha, K.S.R. College of Engineering, India
Assist. Prof. Kavita Choudhary, ITM University, Gurgaon
Dr. Mehrdad Jalali, Azad University, Mashhad, Iran
Megha Goel, Shamli Institute of Engineering and Technology, Shamli, India
Mr. Chi-Hua Chen, Institute of Information Management, National Chiao-Tung University, Taiwan (R.O.C.)
Assoc. Prof. A. Rajendran, RVS College of Engineering and Technology, India
Assist. Prof. S. Jaganathan, RVS College of Engineering and Technology, India
Assoc. Prof. (Dr.) A S N Chakravarthy, JNTUK University College of Engineering Vizianagaram (State University)
Assist. Prof. Deepshikha Patel, Technocrat Institute of Technology, India
Assist. Prof. Maram Balajee, GMRIT, India
Assist. Prof. Monika Bhatnagar, TIT, India
Prof. Gaurang Panchal, Charotar University of Science & Technology, India
Prof. Anand K. Tripathi, Computer Society of India
Prof. Jyoti Chaudhary, High Performance Computing Research Lab, India
Assist. Prof. Supriya Raheja, ITM University, India

Dr. Pankaj Gupta, Microsoft Corporation, U.S.A.
Assist. Prof. Panchamukesh Chandaka, Hyderabad Institute of Tech. & Management, India
Prof. Mohan H.S, SJB Institute Of Technology, India
Mr. Hossein Malekinezhad, Islamic Azad University, Iran
Mr. Zatin Gupta, Universti Malaysia, Malaysia
Assist. Prof. Amit Chauhan, Phonics Group of Institutions, India
Assist. Prof. Ajal A. J., METS School Of Engineering, India
Mrs. Omowunmi Omobola Adeyemo, University of Ibadan, Nigeria
Dr. Bharat Bhushan Agarwal, I.F.T.M. University, India
Md. Nazrul Islam, University of Western Ontario, Canada
Tushar Kanti, L.N.C.T, Bhopal, India
Er. Aumreesh Kumar Saxena, SIRTs College Bhopal, India
Mr. Mohammad Monirul Islam, Daffodil International University, Bangladesh
Dr. Kashif Nisar, University Utara Malaysia, Malaysia
Dr. Wei Zheng, Rutgers Univ/ A10 Networks, USA
Associate Prof. Rituraj Jain, Vyas Institute of Engg & Tech, Jodhpur – Rajasthan
Assist. Prof. Apoorvi Sood, I.T.M. University, India
Dr. Kayhan Zrar Ghafoor, University Technology Malaysia, Malaysia
Mr. Swapnil Sonar, Truba Institute College of Engineering & Technology, Indore, India
Ms. Yogita Gigras, I.T.M. University, India
Associate Prof. Neelima Sadineni, Pydha Engineering College, India Pydha Engineering College
Assist. Prof. K. Deepika Rani, HITAM, Hyderabad
Ms. Shikha Maheshwari, Jaipur Engineering College & Research Centre, India
Prof. Dr V S Giridhar Akula, Avanthi's Scientific Tech. & Research Academy, Hyderabad
Prof. Dr.S.Saravanan, Muthayammal Engineering College, India
Mr. Mehdi Golsorkhatabar Amiri, Islamic Azad University, Iran
Prof. Amit Sadanand Savyanavar, MITCOE, Pune, India
Assist. Prof. P.Oliver Jayaprakash, Anna University, Chennai
Assist. Prof. Ms. Sujata, ITM University, Gurgaon, India
Dr. Asoke Nath, St. Xavier's College, India
Mr. Masoud Rafighi, Islamic Azad University, Iran
Assist. Prof. RamBabu Pemula, NIMRA College of Engineering & Technology, India
Assist. Prof. Ms Rita Chhikara, ITM University, Gurgaon, India
Mr. Sandeep Maan, Government Post Graduate College, India
Prof. Dr. S. Muralidharan, Mepco Schlenk Engineering College, India
Associate Prof. T.V.Sai Krishna, QIS College of Engineering and Technology, India
Mr. R. Balu, Bharathiar University, Coimbatore, India
Assist. Prof. Shekhar. R, Dr.SM College of Engineering, India
Prof. P. Senthilkumar, Vivekanandha Institue of Engineering and Technology for Woman, India
Mr. M. Kamarajan, PSNA College of Engineering & Technology, India
Dr. Angajala Srinivasa Rao, Jawaharlal Nehru Technical University, India
Assist. Prof. C. Venkatesh, A.I.T.S, Rajampet, India
Mr. Afshin Rezakhani Roozbahani, Ayatollah Boroujerdi University, Iran
Mr. Laxmi chand, SCTL, Noida, India
Dr. Dr. Abdul Hannan, Vivekanand College, Aurangabad
Prof. Mahesh Panchal, KITRC, Gujarat
Dr. A. Subramani, K.S.R. College of Engineering, Tiruchengode

Assist. Prof. Prakash M, Rajalakshmi Engineering College, Chennai, India
Assist. Prof. Akhilesh K Sharma, Sir Padampat Singhanian University, India
Ms. Varsha Sahni, Guru Nanak Dev Engineering College, Ludhiana, India
Associate Prof. Trilochan Rout, NM Institute of Engineering and Technology, India
Mr. Srikanta Kumar Mohapatra, NMIET, Orissa, India
Mr. Waqas Haider Bangyal, Iqra University Islamabad, Pakistan
Dr. S. Vijayaragavan, Christ College of Engineering and Technology, Pondicherry, India
Prof. Elbouchari Mohamed, University Mohammed First, Oujda, Morocco
Dr. Muhammad Asif Khan, King Faisal University, Saudi Arabia
Dr. Nagy Ramadan Darwish Omran, Cairo University, Egypt.
Assistant Prof. Anand Nayyar, KCL Institute of Management and Technology, India
Mr. G. Premsankar, Ericsson, India
Assist. Prof. T. Hemalatha, VELS University, India
Prof. Tejaswini Apte, University of Pune, India
Dr. Edmund Ng Giap Weng, Universiti Malaysia Sarawak, Malaysia
Mr. Mahdi Nouri, Iran University of Science and Technology, Iran
Associate Prof. S. Asif Hussain, Annamacharya Institute of technology & Sciences, India
Mrs. Kavita Pabreja, Maharaja Surajmal Institute (an affiliate of GGSIP University), India
Mr. Vorugunti Chandra Sekhar, DA-IICT, India
Mr. Muhammad Najmi Ahmad Zabidi, Universiti Teknologi Malaysia, Malaysia
Dr. Aderemi A. Atayero, Covenant University, Nigeria
Assist. Prof. Osama Sohaib, Balochistan University of Information Technology, Pakistan
Assist. Prof. K. Suresh, Annamacharya Institute of Technology and Sciences, India
Mr. Hassen Mohammed Abdullaah Alsafi, International Islamic University Malaysia (IIUM) Malaysia
Mr. Robail Yasrab, Virtual University of Pakistan, Pakistan
Mr. R. Balu, Bharathiar University, Coimbatore, India
Prof. Anand Nayyar, KCL Institute of Management and Technology, Jalandhar
Assoc. Prof. Vivek S Deshpande, MIT College of Engineering, India
Prof. K. Saravanan, Anna university Coimbatore, India
Dr. Ravendra Singh, MJP Rohilkhand University, Bareilly, India
Mr. V. Mathivanan, IBRA College of Technology, Sultanate of OMAN
Assoc. Prof. S. Asif Hussain, AITS, India
Assist. Prof. C. Venkatesh, AITS, India
Mr. Sami Ulhaq, SZABIST Islamabad, Pakistan
Dr. B. Justus Rabi, Institute of Science & Technology, India
Mr. Anuj Kumar Yadav, Dehradun Institute of technology, India
Mr. Alejandro Mosquera, University of Alicante, Spain
Assist. Prof. Arjun Singh, Sir Padampat Singhanian University (SPSU), Udaipur, India
Dr. Smriti Agrawal, JB Institute of Engineering and Technology, Hyderabad
Assist. Prof. Swathi Sambangi, Visakha Institute of Engineering and Technology, India
Ms. Prabhjot Kaur, Guru Gobind Singh Indraprastha University, India
Mrs. Samaher AL-Hothali, Yanbu University College, Saudi Arabia
Prof. Rajneeshkaur Bedi, MIT College of Engineering, Pune, India
Mr. Hassen Mohammed Abdullaah Alsafi, International Islamic University Malaysia (IIUM)
Dr. Wei Zhang, Amazon.com, Seattle, WA, USA
Mr. B. Santhosh Kumar, C S I College of Engineering, Tamil Nadu
Dr. K. Reji Kumar, N S S College, Pandalam, India

Assoc. Prof. K. Seshadri Sastry, EILM University, India
Mr. Kai Pan, UNC Charlotte, USA
Mr. Ruikar Sachin, SGGSIET, India
Prof. (Dr.) Vinodani Katiyar, Sri Ramswaroop Memorial University, India
Assoc. Prof., M. Giri, Sreenivasa Institute of Technology and Management Studies, India
Assoc. Prof. Labib Francis Gergis, Misr Academy for Engineering and Technology (MET), Egypt
Assist. Prof. Amanpreet Kaur, ITM University, India
Assist. Prof. Anand Singh Rajawat, Shri Vaishnav Institute of Technology & Science, Indore
Mrs. Hadeel Saleh Haj Aliwi, Universiti Sains Malaysia (USM), Malaysia
Dr. Abhay Bansal, Amity University, India
Dr. Mohammad A. Mezher, Fahad Bin Sultan University, KSA
Assist. Prof. Nidhi Arora, M.C.A. Institute, India
Prof. Dr. P. Suresh, Karpagam College of Engineering, Coimbatore, India
Dr. Kannan Balasubramanian, Mepco Schlenk Engineering College, India
Dr. S. Sankara Gomathi, Panimalar Engineering college, India
Prof. Anil kumar Suthar, Gujarat Technological University, L.C. Institute of Technology, India
Assist. Prof. R. Hubert Rajan, NOORUL ISLAM UNIVERSITY, India
Assist. Prof. Dr. Jyoti Mahajan, College of Engineering & Technology
Assist. Prof. Homam Reda El-Taj, College of Network Engineering, Saudi Arabia & Malaysia
Mr. Bijan Paul, Shahjalal University of Science & Technology, Bangladesh
Assoc. Prof. Dr. Ch V Phani Krishna, KL University, India
Dr. Vishal Bhatnagar, Ambedkar Institute of Advanced Communication Technologies & Research, India
Dr. Lamri LAOUAMER, Al Qassim University, Dept. Info. Systems & European University of Brittany, Dept. Computer Science, UBO, Brest, France
Prof. Ashish Babanrao Sasankar, G.H.Raisoni Institute Of Information Technology, India
Prof. Pawan Kumar Goel, Shamli Institute of Engineering and Technology, India
Mr. Ram Kumar Singh, S.V Subharti University, India
Assistant Prof. Sunish Kumar O S, Amaljiyothi College of Engineering, India
Dr Sanjay Bhargava, Banasthali University, India
Mr. Pankaj S. Kulkarni, AVEW's Shatabdi Institute of Technology, India
Mr. Roohollah Etemadi, Islamic Azad University, Iran
Mr. Oloruntoyin Sefiu Taiwo, Emmanuel Alayande College Of Education, Nigeria
Mr. Sumit Goyal, National Dairy Research Institute, India
Mr Jaswinder Singh Dilawari, Geeta Engineering College, India
Prof. Raghuraj Singh, Harcourt Butler Technological Institute, Kanpur
Dr. S.K. Mahendran, Anna University, Chennai, India
Dr. Amit Wason, Hindustan Institute of Technology & Management, Punjab
Dr. Ashu Gupta, Apeejay Institute of Management, India
Assist. Prof. D. Asir Antony Gnana Singh, M.I.E.T Engineering College, India
Mrs Mina Farmanbar, Eastern Mediterranean University, Famagusta, North Cyprus
Mr. Maram Balajee, GMR Institute of Technology, India
Mr. Moiz S. Ansari, Isra University, Hyderabad, Pakistan
Mr. Adebayo, Olawale Surajudeen, Federal University of Technology Minna, Nigeria
Mr. Jasvir Singh, University College Of Engg., India
Mr. Vivek Tiwari, MANIT, Bhopal, India
Assoc. Prof. R. Navaneethakrishnan, Bharathiyar College of Engineering and Technology, India
Mr. Somdip Dey, St. Xavier's College, Kolkata, India

Mr. Souleymane Balla-Arabé, Xi'an University of Electronic Science and Technology, China
Mr. Mahabub Alam, Rajshahi University of Engineering and Technology, Bangladesh
Mr. Sathyapraksh P., S.K.P Engineering College, India
Dr. N. Karthikeyan, SNS College of Engineering, Anna University, India
Dr. Binod Kumar, JSPM's, Jayawant Technical Campus, Pune, India
Assoc. Prof. Dinesh Goyal, Suresh Gyan Vihar University, India
Mr. Md. Abdul Ahad, K L University, India
Mr. Vikas Bajpai, The LNM IIT, India
Dr. Manish Kumar Anand, Salesforce (R & D Analytics), San Francisco, USA
Assist. Prof. Dheeraj Murari, Kumaon Engineering College, India
Assoc. Prof. Dr. A. Muthukumaravel, VELS University, Chennai
Mr. A. Siles Balasingh, St.Joseph University in Tanzania, Tanzania
Mr. Ravindra Daga Badgujar, R C Patel Institute of Technology, India
Dr. Preeti Khanna, SVKM's NMIMS, School of Business Management, India
Mr. Kumar Dayanand, Cambridge Institute of Technology, India
Dr. Syed Asif Ali, SMI University Karachi, Pakistan
Prof. Pallvi Pandit, Himachal Pradesh University, India
Mr. Ricardo Verschueren, University of Gloucestershire, UK
Assist. Prof. Mamta Juneja, University Institute of Engineering and Technology, Panjab University, India
Assoc. Prof. P. Surendra Varma, NRI Institute of Technology, JNTU Kakinada, India
Assist. Prof. Gaurav Shrivastava, RGPV / SVITS Indore, India
Dr. S. Sumathi, Anna University, India
Assist. Prof. Ankita M. Kapadia, Charotar University of Science and Technology, India
Mr. Deepak Kumar, Indian Institute of Technology (BHU), India
Dr. Dr. Rajan Gupta, GGSIP University, New Delhi, India
Assist. Prof M. Anand Kumar, Karpagam University, Coimbatore, India
Mr. Mr Arshad Mansoor, Pakistan Aeronautical Complex
Mr. Kapil Kumar Gupta, Ansal Institute of Technology and Management, India
Dr. Neeraj Tomer, SINE International Institute of Technology, Jaipur, India
Assist. Prof. Trunal J. Patel, C.G.Patel Institute of Technology, Uka Tarsadia University, Bardoli, Surat
Mr. Sivakumar, Codework solutions, India
Mr. Mohammad Sadegh Mirzaei, PGNR Company, Iran
Dr. Gerard G. Dumancas, Oklahoma Medical Research Foundation, USA
Mr. Varadala Sridhar, Varadhaman College Engineering College, Affiliated To JNTU, Hyderabad
Assist. Prof. Manoj Dhawan, SVITS, Indore
Assoc. Prof. Chitreshh Banerjee, Suresh Gyan Vihar University, Jaipur, India
Dr. S. Santhi, SCSVMV University, India
Mr. Davood Mohammadi Souran, Ministry of Energy of Iran, Iran
Mr. Shamim Ahmed, Bangladesh University of Business and Technology, Bangladesh
Mr. Sandeep Reddivari, Mississippi State University, USA
Assoc. Prof. Ousmane Thiare, Gaston Berger University, Senegal
Dr. Hazra Imran, Athabasca University, Canada
Dr. Setu Kumar Chaturvedi, Technocrats Institute of Technology, Bhopal, India
Mr. Mohd Dilshad Ansari, Jaypee University of Information Technology, India
Ms. Jaspreet Kaur, Distance Education LPU, India
Dr. D. Nagarajan, Salalah College of Technology, Sultanate of Oman
Dr. K.V.N.R.Sai Krishna, S.V.R.M. College, India

Mr. Himanshu Pareek, Center for Development of Advanced Computing (CDAC), India
Mr. Khaldi Amine, Badji Mokhtar University, Algeria
Mr. Mohammad Sadegh Mirzaei, Scientific Applied University, Iran
Assist. Prof. Khyati Chaudhary, Ram-eesh Institute of Engg. & Technology, India
Mr. Sanjay Agal, Pacific College of Engineering Udaipur, India
Mr. Abdul Mateen Ansari, King Khalid University, Saudi Arabia
Dr. H.S. Behera, Veer Surendra Sai University of Technology (VSSUT), India
Dr. Shrikant Tiwari, Shri Shankaracharya Group of Institutions (SSGI), India
Prof. Ganesh B. Regulwar, Shri Shankarprasad Agnihotri College of Engg, India
Prof. Pinnamaneni Bhanu Prasad, Matrix vision GmbH, Germany
Dr. Shrikant Tiwari, Shri Shankaracharya Technical Campus (SSTC), India
Dr. Siddesh G.K., : Dayananada Sagar College of Engineering, Bangalore, India
Dr. Nadir Bouchama, CERIST Research Center, Algeria
Dr. R. Sathishkumar, Sri Venkateswara College of Engineering, India
Assistant Prof (Dr.) Mohamed Moussaoui, Abdelmalek Essaadi University, Morocco
Dr. S. Malathi, Panimalar Engineering College, Chennai, India
Dr. V. Subedha, Panimalar Institute of Technology, Chennai, India
Dr. Prashant Panse, Swami Vivekanand College of Engineering, Indore, India
Dr. Hamza Aldabbas, Al-Balqa'a Applied University, Jordan
Dr. G. Rasitha Banu, Vel's University, Chennai
Dr. V. D. Ambeth Kumar, Panimalar Engineering College, Chennai
Prof. Anuranjan Misra, Bhagwant Institute of Technology, Ghaziabad, India
Ms. U. Sinthuja, PSG college of arts & science, India
Dr. Ehsan Saradar Torshizi, Urmia University, Iran
Dr. Shamneesh Sharma, APG Shimla University, Shimla (H.P.), India
Assistant Prof. A. S. Syed Navaz, Muthayammal College of Arts & Science, India
Assistant Prof. Ranjit Panigrahi, Sikkim Manipal Institute of Technology, Majitar, Sikkim
Dr. Khaled Eskaf, Arab Academy for Science ,Technology & Maritime Transportation, Egypt
Dr. Nishant Gupta, University of Jammu, India
Assistant Prof. Nagarajan Sankaran, Annamalai University, Chidambaram, Tamilnadu, India
Assistant Prof. Tribikram Pradhan, Manipal Institute of Technology, India
Dr. Nasser Lotfi, Eastern Mediterranean University, Northern Cyprus
Dr. R. Manavalan, K S Rangasamy college of Arts and Science, Tamilnadu, India
Assistant Prof. P. Krishna Sankar, K S Rangasamy college of Arts and Science, Tamilnadu, India
Dr. Rahul Malik, Cisco Systems, USA
Dr. S. C. Lingareddy, ALPHA College of Engineering, India
Assistant Prof. Mohammed Shuaib, Interat University, Lucknow, India
Dr. Sachin Yele, Sanghvi Institute of Management & Science, India
Dr. T. Thambidurai, Sun Univercell, Singapore
Prof. Anandkumar Telang, BKIT, India
Assistant Prof. R. Poorvadevi, SCSVMV University, India
Dr Uttam Mande, Gitam University, India
Dr. Poornima Girish Naik, Shahu Institute of Business Education and Research (SIBER), India
Prof. Md. Abu Kausar, Jaipur National University, Jaipur, India
Dr. Mohammed Zuber, AISECT University, India
Prof. Kalum Priyanath Udagepola, King Abdulaziz University, Saudi Arabia
Dr. K. R. Ananth, Velalar College of Engineering and Technology, India

Assistant Prof. Sanjay Sharma, Roorkee Engineering & Management Institute Shamli (U.P), India
Assistant Prof. Panem Charan Arur, Priyadarshini Institute of Technology, India
Dr. Ashwak Mahmood muhsen alabaichi, Karbala University / College of Science, Iraq
Dr. Urmila Shrawankar, G H Raison College of Engineering, Nagpur (MS), India
Dr. Krishan Kumar Paliwal, Panipat Institute of Engineering & Technology, India
Dr. Mukesh Negi, Tech Mahindra, India
Dr. Anuj Kumar Singh, Amity University Gurgaon, India
Dr. Babar Shah, Gyeongsang National University, South Korea
Assistant Prof. Jayprakash Upadhyay, SRI-TECH Jabalpur, India
Assistant Prof. Varadala Sridhar, Vidya Jyothi Institute of Technology, India
Assistant Prof. Parameshachari B D, KSIT, Bangalore, India
Assistant Prof. Ankit Garg, Amity University, Haryana, India
Assistant Prof. Rajashe Karappa, SDMCET, Karnataka, India
Assistant Prof. Varun Jasuja, GNIT, India
Assistant Prof. Sonal Honale, Abha Gaikwad Patil College of Engineering Nagpur, India
Dr. Pooja Choudhary, CT Group of Institutions, NIT Jalandhar, India
Dr. Faouzi Hidoussi, UHL Batna, Algeria
Dr. Naseer Ali Hussein, Wasit University, Iraq
Assistant Prof. Vinod Kumar Shukla, Amity University, Dubai
Dr. Ahmed Farouk Metwaly, K L University
Mr. Mohammed Noaman Murad, Cihan University, Iraq
Dr. Suxing Liu, Arkansas State University, USA
Dr. M. Gomathi, Velalar College of Engineering and Technology, India
Assistant Prof. Sumardiono, College PGRI Blitar, Indonesia
Dr. Latika Kharb, Jagan Institute of Management Studies (JIMS), Delhi, India
Associate Prof. S. Raja, Pauls College of Engineering and Technology, Tamilnadu, India
Assistant Prof. Seyed Reza Pakize, Shahid Sani High School, Iran
Dr. Thiyagu Nagaraj, University-INOUE, India
Assistant Prof. Noreen Sarai, Harare Institute of Technology, Zimbabwe
Assistant Prof. Gajanand Sharma, Suresh Gyan Vihar University Jaipur, Rajasthan, India
Assistant Prof. Mapari Vikas Prakash, Siddhant COE, Sudumbare, Pune, India
Dr. Devesh Katiyar, Shri Ramswaroop Memorial University, India
Dr. Shenshen Liang, University of California, Santa Cruz, US
Assistant Prof. Mohammad Abu Omar, Limkokwing University of Creative Technology- Malaysia
Mr. Snehasis Banerjee, Tata Consultancy Services, India
Assistant Prof. Kibona Lusekelo, Ruaha Catholic University (RUCU), Tanzania
Assistant Prof. Adib Kabir Chowdhury, University College Technology Sarawak, Malaysia
Dr. Ying Yang, Computer Science Department, Yale University, USA
Dr. Vinay Shukla, Institute Of Technology & Management, India
Dr. Liviu Octavian Maftciu-Scai, West University of Timisoara, Romania
Assistant Prof. Rana Khudhair Abbas Ahmed, Al-Rafidain University College, Iraq
Assistant Prof. Nitin A. Naik, S.R.T.M. University, India
Dr. Timothy Powers, University of Hertfordshire, UK
Dr. S. Prasath, Bharathiar University, Erode, India
Dr. Ritu Shrivastava, SIRTIS Bhopal, India
Prof. Rohit Shrivastava, Mittal Institute of Technology, Bhopal, India
Dr. Gianina Mihai, Dunarea de Jos" University of Galati, Romania

Assistant Prof. Ms. T. Kalai Selvi, Erode Sengunthar Engineering College, India
Assistant Prof. Ms. C. Kavitha, Erode Sengunthar Engineering College, India
Assistant Prof. K. Sinivasamoorthi, Erode Sengunthar Engineering College, India
Assistant Prof. Mallikarjun C Sarsamba Bheemna Khandre Institute Technology, Bhalki, India
Assistant Prof. Vishwanath Chikaraddi, Veermata Jijabai technological Institute (Central Technological Institute), India
Assistant Prof. Dr. Ikinderpal Singh, Trai Shatabdi GGS Khalsa College, India
Assistant Prof. Mohammed Noaman Murad, Cihan University, Iraq
Professor Yousef Farhaoui, Moulay Ismail University, Errachidia, Morocco
Dr. Parul Verma, Amity University, India
Professor Yousef Farhaoui, Moulay Ismail University, Errachidia, Morocco
Assistant Prof. Madhavi Dhingra, Amity University, Madhya Pradesh, India
Assistant Prof.. G. Selvavinayagam, SNS College of Technology, Coimbatore, India
Assistant Prof. Madhavi Dhingra, Amity University, MP, India
Professor Kartheesan Log, Anna University, Chennai
Professor Vasudeva Acharya, Shri Madhwa vadiraja Institute of Technology, India
Dr. Asif Iqbal Hajamydeen, Management & Science University, Malaysia
Assistant Prof., Mahendra Singh Meena, Amity University Haryana
Assistant Professor Manjeet Kaur, Amity University Haryana
Dr. Mohamed Abd El-Basset Matwalli, Zagazig University, Egypt
Dr. Ramani Kannan, Universiti Teknologi PETRONAS, Malaysia
Assistant Prof. S. Jagadeesan Subramaniam, Anna University, India
Assistant Prof. Dharmendra Choudhary, Tripura University, India
Assistant Prof. Deepika Vodnala, SR Engineering College, India
Dr. Kai Cong, Intel Corporation & Computer Science Department, Portland State University, USA
Dr. Kailas R Patil, Vishwakarma Institute of Information Technology (VIIT), India
Dr. Omar A. Alzubi, Faculty of IT / Al-Balqa Applied University, Jordan
Assistant Prof. Kareemullah Shaik, Nimra Institute of Science and Technology, India
Assistant Prof. Chirag Modi, NIT Goa
Dr. R. Ramkumar, Nandha Arts And Science College, India
Dr. Priyadarshini Vydialingam, Harathiar University, India
Dr. P. S. Jagadeesh Kumar, DBIT, Bangalore, Karnataka
Dr. Vikas Thada, AMITY University, Pachgaon
Dr. T. A. Ashok Kumar, Institute of Management, Christ University, Bangalore
Dr. Shaheera Rashwan, Informatics Research Institute
Dr. S. Preetha Gunasekar, Bharathiyar University, India
Asst Professor Sameer Dev Sharma, Uttaranchal University, Dehradun
Dr. Zhihan Iv, Chinese Academy of Science, China
Dr. Ikinderpal Singh, Trai Shatabdi GGS Khalsa College, Amritsar
Dr. Umar Ruhi, University of Ottawa, Canada
Dr. Jasmin Cosic, University of Bihac, Bosnia and Herzegovina
Dr. Homam Reda El-Taj, University of Tabuk, Kingdom of Saudi Arabia
Dr. Mostafa Ghobaei Arani, Islamic Azad University, Iran
Dr. Ayyasamy Ayyanar, Annamalai University, India
Dr. Selvakumar Manickam, Universiti Sains Malaysia, Malaysia
Dr. Murali Krishna Namana, GITAM University, India
Dr. Smriti Agrawal, Chaitanya Bharathi Institute of Technology, Hyderabad, India
Professor Vimalathithan Rathinasabapathy, Karpagam College Of Engineering, India

Dr. Sushil Chandra Dimri, Graphic Era University, India
Dr. Dinh-Sinh Mai, Le Quy Don Technical University, Vietnam
Dr. S. Rama Sree, Aditya Engg. College, India
Dr. Ehab T. Alnfwawy, Sadat Academy, Egypt
Dr. Patrick D. Cerna, Haramaya University, Ethiopia
Dr. Vishal Jain, Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), India
Associate Prof. Dr. Jiliang Zhang, North Eastern University, China
Dr. Sharefa Murad, Middle East University, Jordan
Dr. Ajeet Singh Poonia, Govt. College of Engineering & technology, Rajasthan, India
Dr. Vahid Esmaealzadeh, University of Science and Technology, Iran
Dr. Jacek M. Czerniak, Casimir the Great University in Bydgoszcz, Institute of Technology, Poland
Associate Prof. Anisur Rehman Nasir, Jamia Millia Islamia University
Assistant Prof. Imran Ahmad, COMSATS Institute of Information Technology, Pakistan
Professor Ghulam Qasim, Preston University, Islamabad, Pakistan
Dr. Parameshachari B D, GSSS Institute of Engineering and Technology for Women
Dr. Wencan Luo, University of Pittsburgh, US
Dr. Musa PEKER, Faculty of Technology, Mugla Sitki Kocman University, Turkey
Dr. Gunasekaran Shanmugam, Anna University, India
Dr. Binh P. Nguyen, National University of Singapore, Singapore
Dr. Rajkumar Jain, Indian Institute of Technology Indore, India
Dr. Imtiaz Ali Halepoto, QUEST Nawabshah, Pakistan
Dr. Shaligram Prajapat, Devi Ahilya University Indore India
Dr. Sunita Singhal, Birla Institute of Technology and Science, Pilani, India
Dr. Ijaz Ali Shoukat, King Saud University, Saudi Arabia
Dr. Anuj Gupta, IKG Punjab Technical University, India
Dr. Sonali Saini, IES-IPS Academy, India
Dr. Krishan Kumar, Moti Lal Nehru National Institute of Technology, Allahabad, India
Dr. Z. Faizal Khan, College of Engineering, Shaqra University, Kingdom of Saudi Arabia
Prof. M. Padmavathamma, S.V. University Tirupati, India
Prof. A. Velayudham, Cape Institute of Technology, India
Prof. Seifeidne Kadry, American University of the Middle East
Dr. J. Durga Prasad Rao, Pt. Ravishankar Shukla University, Raipur
Assistant Prof. Najam Hasan, Dhofar University
Dr. G. Suseendran, Vels University, Pallavaram, Chennai
Prof. Ankit Faldu, Gujarat Technological University- Atmiya Institute of Technology and Science
Dr. Ali Habiboghli, Islamic Azad University
Dr. Deepak Dembla, JECRC University, Jaipur, India
Dr. Pankaj Rajan, Walmart Labs, USA
Assistant Prof. Radoslava Kraveva, South-West University "Neofit Rilski", Bulgaria
Assistant Prof. Medhavi Shriwas, Shri vaishnav institute of Technology, India
Associate Prof. Sedat Akleylek, Ondokuz Mayıs University, Turkey
Dr. U.V. Arivazhagu, Kingston Engineering College Affiliated To Anna University, India
Dr. Touseef Ali, University of Engineering and Technology, Taxila, Pakistan
Assistant Prof. Naren Jeeva, SASTRA University, India
Dr. Riccardo Colella, University of Salento, Italy
Dr. Enache Maria Cristina, University of Galati, Romania
Dr. Senthil P, Kuringi College of Arts & Science, India

Dr. Hasan Ashrafi-rizi, Isfahan University of Medical Sciences, Isfahan, Iran
Dr. Mazhar Malik, Institute of Southern Punjab, Pakistan
Dr. Yajie Miao, Carnegie Mellon University, USA
Dr. Kamran Shaukat, University of the Punjab, Pakistan
Dr. Sasikaladevi N., SASTRA University, India
Dr. Ali Asghar Rahmani Hosseinabadi, Islamic Azad University Ayatollah Amoli Branch, Amol, Iran
Dr. Velin Kralev, South-West University "Neofit Rilski", Blagoevgrad, Bulgaria
Dr. Marius Iulian Mihailescu, LUMINA - The University of South-East Europe
Dr. Sriramula Nagaprasad, S.R.R.Govt.Arts & Science College, Karimnagar, India
Prof (Dr.) Namrata Dhanda, Dr. APJ Abdul Kalam Technical University, Lucknow, India
Dr. Javed Ahmed Mahar, Shah Abdul Latif University, Khairpur Mir's, Pakistan
Dr. B. Narendra Kumar Rao, Sree Vidyanikethan Engineering College, India
Dr. Shahzad Anwar, University of Engineering & Technology Peshawar, Pakistan
Dr. Basit Shahzad, King Saud University, Riyadh - Saudi Arabia
Dr. Nilamadhab Mishra, Chang Gung University
Dr. Sachin Kumar, Indian Institute of Technology Roorkee
Dr. Santosh Nanda, Biju-Pattnaik University of Technology
Dr. Sherzod Turaev, International Islamic University Malaysia
Dr. Yilun Shang, Tongji University, Department of Mathematics, Shanghai, China
Dr. Nuzhat Shaikh, Modern Education society's College of Engineering, Pune, India
Dr. Parul Verma, Amity University, Lucknow campus, India
Dr. Rachid Alaoui, Agadir Ibn Zohr University, Agadir, Morocco
Dr. Dharmendra Patel, Charotar University of Science and Technology, India
Dr. Dong Zhang, University of Central Florida, USA
Dr. Kennedy Chinedu Okafor, Federal University of Technology Owerri, Nigeria
Prof. C Ram Kumar, Dr NGP Institute of Technology, India
Dr. Sandeep Gupta, GGS IP University, New Delhi, India
Dr. Shahanawaj Ahamad, University of Ha'il, Ha'il City, Ministry of Higher Education, Kingdom of Saudi Arabia
Dr. Najeed Ahmed Khan, NED University of Engineering & Technology, India
Dr. Sajid Ullah Khan, Universiti Malaysia Sarawak, Malaysia
Dr. Muhammad Asif, National Textile University Faisalabad, Pakistan
Dr. Yu BI, University of Central Florida, Orlando, FL, USA
Dr. Brijendra Kumar Joshi, Research Center, Military College of Telecommunication Engineering, India
Prof. Dr. Nak Eun Cho, Pukyong National University, Korea
Prof. Wasim Ul-Haq, Faculty of Science, Majmaah University, Saudi Arabia
Dr. Mohsan Raza, G.C University Faisalabad, Pakistan
Dr. Syed Zakar Hussain Bukhari, National Science and Technology Azad Jamu Kashmir, Pakistan
Dr. Ruksar Fatima, KBN College of Engineering, Gulbarga, Karnataka, India
Associate Professor S. Karpagavalli, Department of Computer Science, PSGR Krishnammal College for Women
Coimbatore, Tamilnadu, India
Dr. Bushra Mohamed Elamin Elhaim, Prince Sattam bin Abdulaziz University, Saudi Arabia
Dr. Shamik Tiwari, Department of CSE, CET, Mody University, Lakshmangarh
Dr. Rohit Raja, Faculty of Engineering and Technology, Shri Shankaracharya Group of Institutions, India
Prof. Dr. Aqeel-ur-Rehman, Department of Computing, HIET, FEST, Hamdard University, Pakistan
Dr. Nageswara Rao Moparthi, Velagapudi Ramakrishna Siddhartha Engineering College, India
Dr. Mohd Muqeem, Department of Computer Application, Integral University, Lucknow, India
Dr. Zeeshan Bhatti, Institute of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan

Dr. Emrah Irmak, Biomedical Engineering Department, Karabuk University, Turkey

Dr. Fouad Abdulameer salman, School of Informatics and Applied Mathematics, Universiti Malaysia Terengganu

Dr. N. Prasath, Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Arasur, Coimbatore

Dr. Hasan Ashrafi-rizi, Health Information Technology Research Center, Isfahan University of Medical Sciences, Hezar Jerib Avenue, Isfahan, Iran

Dr. N. Sasikaladevi, School of Computing, SASTRA University, Thirumalisamudram, Tamilnadu, India.

Dr. Anchit Bijalwan, Arba Minch University, Ethiopia

Dr. K. Sathishkumar, BlueCrest University College, Accra North, Ghana, West Africa

Dr. Dr. Parameshachari B D, GSSS Institute of Engineering and Technology for Women, Affiliated to Visvesvaraya Technological University, Belagavi

Dr. C. Shoba Bindu, Dept. of CSE, JNTUA College of Engineering, India

Dr. M. Inbavalli, ER. Perumal Manimekalai College of Engineering, Hosur, Tamilnadu, India

Dr. Vidya Sagar Ponnamm, Dept. of IT, Velagapudi Ramakrishna Siddhartha Engineering College, India

Dr. Kelvin LO M. F., The Hong Kong Polytechnic University, Hong Kong

Prof. Karimella Vikram, G.H. Raison College of Engineering & Management, Pune, India

Dr. Shajilin Loret J.B., VV College of Engineering, India

Dr. P. Sujatha, Department of Computer Science at Vels University, Chennai

Dr. Vaibhav Sundriyal, Old Dominion University Research Foundation, USA

Dr. Md Masud Rana, Khulna University of Engineering and Technology, Bangladesh

Dr. Gurcharan Singh, Khalsa College Amritsar, Guru Nanak Dev University, Amritsar, India

Dr. Richard Otieno Omollo, Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Kenya

Prof. (Dr) Amit Verma, Computer Science & Engineering, Chandigarh Engineering College, Landran, Mohali, India

Dr. Vidya Sagar Ponnamm, Velagapudi Ramakrishna Siddhartha Engineering College, India

Dr. Bohui Wang, School of Aerospace Science and Technology, Xidian University, P.R. China

Dr. M. Anjan Kumar, Department of Computer Science, Satavahana University, Karimnagar

Dr. Hanumanthappa J., DoS in CS, Uni of Mysuru, Karnataka, India

Dr. Pouya Derakhshan-Barjoei, Dept. of Telecommunication and Engineering, Islamic Azad University, Iran

Dr. Tanweer Alam, Islamic University of Madinah, Dept. of Computer Science, College of Computer and Information System, Al Madinah, Saudi Arabia

Dr. Kumar Keshamoni, Dept. of ECE, Vaagdevi Engineering College, Warangal, Telangana, India

Dr. G. Rajkumar, N.M.S.S.Vellaichamy Nadar College, Madurai, Tamilnadu, India

Dr. P. Mayil Vel Kumar, Karpagam Institute of Technology, Coimbatore, India

Dr. M. Yaswanth Bhanu Murthy, Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

Asst. Prof. Dr. Mehmet Barış TABAKCIOĞLU, Bursa Technical University, Turkey

Dr. Mohd. Muntjir, College of Computers and Information Technology, Taif University, Kingdom of Saudi Arabia

Dr. Sanjay Agal, Aravali Institute of Technical Studies, Udaipur, India

Dr. Shanshan Tuo, xAd Inc., US

Dr. Subhadra Shaw, AKS University, Satna, India

Dr. Piyush Anand, Noida International University, Greater Noida, India

Dr. Brijendra Kumar Joshi, Research Center Military College of Telecommunication Engineering, India

Dr. V. Sreerama Murthy, GMRIT, Rajam, AP, India

Dr. S. Nagarajan, Annamalai University, India

Prof. Pramod Bhausaheb Deshmukh, D. Y. Patil College of Engineering, Akurdi, Pune, India

CALL FOR PAPERS

International Journal of Computer Science and Information Security

IJCSIS 2019-2020

ISSN: 1947-5500

<http://sites.google.com/site/ijcsis/>

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity

Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security, Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc.), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embedded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at <http://sites.google.com/site/ijcsis/authors-notes> .



© IJCSIS PUBLICATION 2019

ISSN 1947 5500

<http://sites.google.com/site/ijcsis/>